MANAGEMENT CONTROL AGREEMENT
RELATING TO BROWARD COUNTY OPERATION OF
THE REGIONAL PUBLIC SAFETY INFRASTRUCTURE

THIS Management Control Agreement is made and entered into by and between: BROWARD COUNTY, a political subdivision of the State of Florida, hereinafter referred to as "COUNTY,"

AND

SHERIFF OF BROWARD COUNTY, hereinafter referred to as "BSO."

WHEREAS, BSO is a Criminal Justice Agency ("CJA") formally recognized as such by both the Federal Bureau of Investigation and the Florida Department of Law Enforcement; and

WHEREAS, on or about January 26, 2010, BSO has entered into a Criminal Justice User Agreement ("the User Agreement") with the Florida Department of Law Enforcement ("FDLE") for the benefit of access to the Criminal Justice Network ("CJNET"), the National Crime Information Center ("NCIC") and the Florida Crime Information Center ("FCIC") and is therefore an authorized user of those technology resources, a copy of which is attached hereto and made part hereof as Exhibit "A"; and

WHEREAS, pursuant to the User Agreement, all state criminal justice agencies with such access must comply with the FBI Criminal Justice Information Services ("CJIS") Security Policy; and

WHEREAS, COUNTY is a Non-Criminal Justice Agency ("NCJA"); and

WHEREAS, COUNTY operates, maintains, and owns the Regional Public Safety Intranet ("RPSI") which includes a portion of computer systems and network infrastructure interfacing directly or indirectly with the State of Florida Criminal Justice Network ("CJNET") for the interstate exchange of criminal history/criminal justice information; and

WHEREAS, BSO and COUNTY desire to enter into a Management Control Agreement..

NOW THEREFORE, in consideration of the mutual terms, conditions, promises, covenants, and payments hereinafter set forth, the parties agree as follows:

I. DEFINITIONS

The following definitions apply unless the context in which the word or phrase is used requires a different definition:

A. BSO CJI- Broward Sheriff's Office Criminal Justice Information
B. CJA- Criminal Justice Agency
C. CJI – Criminal Justice Information
D. CJIS- Criminal Justice Information System
E. CJNET- State of Florida Criminal Justice Network
F. DOJ- Department of Justice
G. FBI- Federal Bureau of Justice
H. FCIC- Florida Crime Information Center
I. FDLE- Florida Department of Law Enforcement
J. NCIC- National Crime Information Center
K. NCJA-Non-Criminal Justice Agency
L. RPSI- Regional Public Safety Intranet
M. TAC- Terminal Agency Coordinator

Exhibits

A – User Agreement between BSO and FDLE
B –CJIS Policy
C- Regional Interlocal Agreement

II. COMPLIANCE WITH CJIS SECURITY POLICIES AND PROCEDURES

A. Pursuant to the Criminal Justice Information Services (CJIS) Security Policy Version 5.1 (dated 07/13/2012), Sections 3.2.2 and 5.1, a copy of which is attached hereto and made part hereof as Exhibit "B", it is agreed that with respect to administration of that portion of the Regional Public Safety Intranet computer systems and network infrastructure computer systems used to administer, collect, store, modify, and exchange BSO CJI, which interfaces directly or indirectly with the Florida CJNET for the intrastate or interstate exchange of criminal history/criminal justice information, BSO shall have the authority, via managed control, to set and enforce:

(1) Priorities.

(2) Standards for the selection, supervision, and termination of personnel from access to BSO CJI,

(3) Policy governing operation of justice systems, computer, access devices, circuits, hubs, routers, firewalls, and any other components, including encryption, that comprise and support a telecommunications network and related criminal justice systems to include but not limited to criminal history record/criminal justice information, insofar as the equipment is used to process or transmit criminal justice systems information guaranteeing the priority, integrity, and availability of service needed by the criminal justice community.

(4) Restriction of unauthorized personnel from access or use of equipment accessing the State network.

(5) Compliance with all CJIS Security Policy rules and regulations in the operation of all information received.

B. Responsibility for management of security control of BSO CJI shall remain with BSO, CJIS Security Policy Version 5.1, Section 3.2. Further, COUNTY shall not restrict BSO's physical access to BSO's CJI.

C. This Agreement covers the overall supervision of all BSO CJI systems, applications, equipment, systems design, programming and operational procedures associated with the development, implementation and maintenance of any BSO system to include NCIC Programs that may be subsequently designed and/or implemented within BSO. COUNTY is not responsible for the cost(s) to upgrade or purchase BSO hardware or software.

D.

E. **BSO RESPONSIBLITIES**

BSO agrees to the following:

1. BSO shall appoint a BSO employee as designee to function as the Terminal Agency Coordinator ("TAC") regarding all issues and services provided in this Agreement and to maintain compliance with CJIS Policy 5.1, Section 3.2.7. BSO shall inform the COUNTY of the name and contact information for the TAC. BSO shall inform the County within 24 hours if the name or contact information for the TAC is changed.

2. BSO shall be responsible for notifying the COUNTY of any subsequent amendments to the CJIS Security Policy.

3. BSO shall, at COUNTY's expense, conduct all background checks of COUNTY personnel, contractors and subcontractors that will have access to BSO CJI for CJIS certification compliance every two (2) years.

4. BSO shall maintain approval for currently authorized COUNTY employees with access to BSO CJI subject to their compliance with CJIS Security Policies and BSO conducted background check for CJIS compliance.

5. BSO will use its best efforts to coordinate the CJIS certification dates for COUNTY staff and contractors accessing BSO CJI.

6. BSO agrees that COUNTY personnel and COUNTY vendors, shall have access to BSO secure locations as may be necessary to perform their job or contract responsibilities, subject to such appropriate and necessary security requirements imposed by BSO.

7. BSO and COUNTY agree to abide by the Change Management Request Process set forth in the Regional Interlocal Agreement, a copy of which is attached hereto and made part hereof as Exhibit "C".

F. **COUNTY RESPONSIBILITIES**
COUNTY agrees to the following:

1. COUNTY agrees to abide by all applicable local, state and federal laws, rules, and regulations, as well as the FBI CJIS Security Policy and rules and regulations of FCI, with regards to accessing FCIC.

2. COUNTY agrees to abide by all applicable terms and conditions of the Criminal Justice User Agreement executed by the FDLE and BSO.

3. COUNTY agrees that in the event BSO provides notification of the adoption, modification or elimination of CJIS policy related to BSO CJI on COUNTY owned equipment, COUNTY shall take immediate steps to implement the adopted, modified or eliminated policy.

4. COUNTY agrees that BSO is the owner of all BSO CJI, and serves as the custodian of said records in accordance to Florida Statutes Chapter 119.

5. COUNTY and BSO understand and agree to the extent any other CJA inputs any data into the records management system, those agencies shall be considered the owners of their respective CJI data and the custodian of said records in accordance to Florida Statutes Chapter 119.

6. COUNTY shall develop and enforce internal policies that restrict unauthorized personnel or contractors from obtaining physical and/or electronic access or use of BSO CJI.

    a. BSO reserves the right to approve, reject and/or modify any COUNTY policies and procedures related to access to BSO CJI.

    b. COUNTY shall provide BSO with a current copy of its policies and procedures related to access to BSO CJI.

7. COUNTY shall maintain and provide to BSO a list of all personnel with access to BSO CJI, including but not limited to, new hires, transfers, and terminations. In the case of the suspension, demotion, transfer, or termination of COUNTY personnel who has/had access to BSO CJI, COUNTY shall notify the BSO TAC in writing as to the procedures taken to restrict or terminate said personnel(s) access within twenty-four (24) hours of the employee disciplinary action.

8. COUNTY shall maintain and provide to BSO a list of all contractors or subcontractors, including the names of any personnel assigned to provide services to the County, with access to BSO CJI. In the event of a termination of an agreement with a contractor, or the termination of a contractor's employee (s), with access to BSO CJI, COUNTY shall immediately restrict all access to BSO CJI and notify the BSO TAC of the action(s) taken to restrict said access.

9. COUNTY shall ensure that any COUNTY employee or COUNTY contractor assigned to support BSO CJI adhere to the DOJ, FBI, CJIS and FDLE requirements regarding CJIS information security including BSO fingerprint-

based background checks and will recognize the authority of BSO regarding electronic and physical access to CJIS and NCIC data.

10. COUNTY will ensure that its contractors or subcontractors having access to BSO CJI are made aware of and comply with the CJIS Security Policy and properly execute the FBI CJIS Security Addendum. COUNTY shall provide BSO with a copy of the executed FBI CJIS Security Addendum within five (5) days of execution.

11. COUNTY employees having access to BSO CJI will meet all CJIS background investigation requirements and obtain any required certifications prior to accessing BSO CJI or CJIS data.

12. COUNTY, following the receipt of information, shall immediately notify the BSO TAC of any employee or contractor with access to BSO CJI that has been arrested or has any pending criminal charges in any jurisdiction within the United States.

13. Upon notification by COUNTY, or through independent verification, BSO shall have the right to, immediately restrict access to BSO CJI for any employee or contractor with access to BSO CJI that has been arrested or has any pending criminal charges in any jurisdiction within the United States. Independent verification by BSO, however, shall not discharge COUNTY's responsibility to notify BSO of a known arrest or pending charge of any COUNTY personnel or contractor with access to BSO CJI.

14. COUNTY shall not grant any NCJA that has not signed a FBI CJIS Security Addendum with access to, applications, equipment, systems design, programming and operational procedures associated with the development, implementation and maintenance of any BSO system to include, but not limited to, NCIC Programs that may be subsequently designed and/or implemented with the BSO and which contain BSO CJI.

15. In the event COUNTY wishes to grant a NCJA access to BSO CJI, COUNTY shall provide BSO with five (5) days notice prior to its execution of the CJIS Security Addendum with the NCJA.

16. COUNTY shall, upon discovery, immediately notify the BSO TAC of any breach, misusage, improper or unauthorized access to BSO CJI.

III. AUDITS & REPORTING

COUNTY agrees to adhere to the following audit and reporting requirements:

1. COUNTY shall immediately provide BSO with access to security logs for event tracking upon request.

2. BSO and COUNTY shall conduct, at such time periods as mutually agreed to, a collaborative internal audit to identify Network security that meets CJIS compliance standards.

3. COUNTY shall identify and define all user roles and the type or level of access that is requested for the respective job function(s).

4. COUNTY shall provide BSO with access to current Network Diagrams upon request.

5. COUNTY's RPSI that contain BSO CJI must comply with physically secure and controlled area locations as per CJIS policy.

6. COUNTY, upon discovery, shall immediately notify the BSO TAC of any BSO CJI computer security incidents including, but not limited to, suspicious events. E-mail notification is an acceptable form of notification.

7. COUNTY agrees that all accounts accessing BSO CJI data must meet password requirements in accordance with the CJIS policy.

8. COUNTY agrees to adhere to all audit requirements imposed by the FBI or FDLE related to BSO CJI as set forth in the audit provisions of the Criminal Justice User Agreement between BSO and FDLE, including but not limited to, permitting an FDLE appointed inspection team to conduct inquiries or site inspections with regard to any allegations or potential security violations, as well as for routing audits.

9. COUNTY agrees to address and/or correct any deficiencies that may be found in an audit(s) conducted by the FBI or FDLE within the timeframe specified in the audit report(s).

10. COUNTY shall provide to BSO for review with a copy of its response(s) to any audit(s) no less than three (3) days prior to the response deadline.

11. COUNTY shall immediately notify BSO in writing of any delay or inability to respond to any audit(s); the reason for the delay or inability to respond; and the expected date of a response to the requesting agency.

IV. TERM & TERMINATION

1. The parties agree that this Management Control Agreement shall be for a term of one (1) year commencing on the date of execution and shall automatically renew on a yearly basis unless terminated by either party as provided herein.

2. Either party may terminate this Management Control Agreement without cause by providing the other party with one hundred and twenty days (120) written notice to the other party. Notice may be delivered by facsimile and the notice will be effective on the date it is given.

3. In the event of a material breach of the terms of this Agreement, and the breach is not cured by the party in breach within a reasonable time period agreed upon by the parties, the non-breaching party may thereafter terminate this Agreement with thirty (30) days written notice to the other party. In the instance where the material breach is committed by COUNTY, BSO shall assume control of all BSO CJI data until such time as the breach is cured by COUNTY.

4. BSO has the management authority and responsibility for compliance with CJIS Policy for BSO CJI. In the event of BSO's termination of this agreement, BSO's assumption of responsibility shall not occur on COUNTY owned RPSI equipment nor shall COUNTY have the obligation to provide any additional funding relating to BSO's assumption of responsibility. Notwithstanding the foregoing, BSO reserves any and all rights, statutory or otherwise, under law including, but not necessarily limited to, BSO's budget and any appeal rights BSO may have regarding funding by COUNTY for BSO's capital, operations and maintenance needs to perform the same services previously provided by COUNTY to BSO as a participant in the RPSI.

V. COSTS

1. Unless otherwise agreed to in writing, each party shall bear its own costs in relation to this Agreement.

2. COUNTY shall solely be responsible for all technical training costs, for COUNTY employees, incurred as a result of the operation of the Regional system.

3. COUNTY shall solely be responsible for all cost(s) associated with background checks and training for COUNTY employees or contractors.

VI. RECORDS

1. Each party shall maintain its records in accordance with the applicable statutory guidelines.

2. Each party shall maintain the confidentiality of its records to the extent that the records are exempt or confidential under Florida or federal law.

VII. NOTICES

Unless otherwise indicated, whenever either party desires to give notice to the other, such notice must be in writing, sent by certified United States Mail, postage prepaid, return receipt requested, or sent by commercial express carrier with acknowledgement of delivery, or by hand delivery with a request for a written receipt of acknowledgment of delivery, addressed to the party for whom it is intended at the place last specified. The place for giving notice shall remain the same as set forth herein until changed in writing in the manner provided in this section. For the present, the parties designate the following:

FOR COUNTY:

Broward County
ATTN: Bertha Henry, County Administrator
115 S. Andrews Ave., Room 409
Fort Lauderdale, FL 33301-1872

FOR BSO:

Broward Sheriff's Office
Attention: Director, Information Technology
2601 W. Broward Blvd.
Fort Lauderdale, FL 33312

With copy to:

Office of the General Counsel
Broward Sheriff's Office
2601 W. Broward Blvd.
Fort Lauderdale, FL 33312

VIII. COMPLIANCE WITH LAWS

COUNTY and BSO shall comply with all federal, state, and local laws, codes, ordinances, rules, and regulations in performing its duties, responsibilities, and obligations pursuant to this Agreement.

IX. INDEMNIFICATION

Nothing herein is intended to serve as a waiver of sovereign immunity by any party nor shall anything included herein be construed as consent to be sued by third parties in any matter arising out of this Agreement or any other contract. COUNTY and BSO are a state agency or political subdivision as defined in Chapter 768.28, Florida Statutes, and shall be fully responsible for the acts and omissions of its agents or employees to the extent permitted by law.

X. VENUE

This Agreement shall be interpreted and construed in accordance with and governed by the laws of the State of Florida. Venue in any proceeding or action arising out of this Agreement shall be in the Seventeenth Judicial Circuit in and for Broward County, Florida.

XI. ENTIRE AGREEMENT

This document incorporates and includes all prior negotiations, correspondence, conversations, agreements and understandings applicable to the matters contained herein and the parties agree that there are no commitments, agreements or understandings concerning the subject matter of this Agreement that are not contained in this document. Accordingly, the parties agree that no deviation from the

terms hereof shall be predicated upon any prior representations or agreements, whether oral or written.

XII. AMENDMENTS

No modification, amendment, or alteration in the terms or conditions contained herein shall be effective unless contained in a written document prepared with the same or similar formality as this Agreement and executed by each party hereto.

XII. WAIVER

The parties agree that each requirement, duty and obligation set forth herein is substantial and important to the formation of this Agreement and, therefore, is a material term hereof. Any party's failure to enforce any provision of this Agreement shall not be deemed a waiver of such provision or modification of this Agreement. A waiver of any breach of a provision of this Agreement shall not be deemed a waiver of any subsequent breach and shall not be construed to be a modification of the terms of this Agreement.

REMAINDER INTENTIONALLY LEFT BLANK

MANAGEMENT CONTROL AGREEMENT RELATING TO BROWARD COUNTY OPERATION OFTHE REGIONAL PUBLIC SAFETY INFRASTRUCTURE

IN WITNESS WHEREOF, the parties have made and executed this Management Control Agreement: BROWARD COUNTY through its BOARD OF COUNTY COMMISSIONERS, signing by and through its County Administrator, duly authorized to execute same and BSO, signing by and through, SCOTT J. ISRAEL, as Sheriff of Broward County, Florida, duly authorized to execute same.

COUNTY

WITNESSES:

BROWARD COUNTY, through its County Administrator

_____

By: _____
County Administrator

_____

____ day of _____, 2013.

Risk Management Division

Jacqueline A. Binns

Risk Insurance and

Contracts Manager

Approved as to form by
Office of County Attorney
Broward County, Florida:

Joni Armstrong Coffey, Broward County Attorney
Governmental Center, Suite 423
115 South Andrews Avenue Fort Lauderdale, Florida 33301
Telephone: (954) 357-7600
Telecopier: (954) 357-7641

By: _____
County Attorney

SHERIFF OF BROWARD COUNTY

By: _____ Date: 2/19/13
SCOTT J. ISRAEL, As Sheriff of Broward County

Approved as to form and legal sufficiency
subject to execution by the parties:

By: _____ Date: 2/7/13
Ronald M. Gunzburger, General Counsel

RECEIVED
JAN 25 2010
CJIS/Information Delivery Team

CRIMINAL JUSTICE USER AGREEMENT

This Agreement, is entered into between the Florida Department of Law Enforcement (hereinafter referred to as FDLE), an agency of the State of Florida with headquarters at 2331 Phillips Road, Tallahassee, Florida and the

Broward Sheriff's Office,

with headquarters at

2601 West Broward Boulevard, Fort Lauderdale, Florida, 33312,

with the primary ORI of: FL0060000, (hereinafter referred to as the User).

Whereas, FDLE is authorized by law to operate and regulate the Criminal Justice Network (hereinafter CJNet) as an intra-agency information and data-sharing network for use by the state's criminal justice agencies;

Whereas, FDLE is authorized by law to establish and operate the Florida Crime Information Center (hereinafter FCIC) for the exchange of information relating to crimes, criminals and criminal activity;

Whereas, FDLE participates in the National Crime Information Center (hereinafter NCIC), a service of the United States Department of Justice, the Interstate Identification Index (hereinafter III), and the International Justice and Public Safety Information Sharing Network (hereinafter NLETS), and serves as Florida's Criminal Justice Information Services (CJIS) Systems Agency (CSA) for the interstate transmission of criminal justice information to and from agencies in Florida and agencies in the continental United States, Alaska, Hawaii, U.S. Virgin Islands, Canada and Puerto Rico;

Whereas, the User requires access to intrastate and interstate criminal justice information systems provided by FDLE through the CJNet in order to effectively discharge its public duties;

Whereas, FDLE will facilitate local law enforcement and other criminal justice agencies' requests to participate in the information services provided on CJNet, provided the User agrees to abide by applicable federal and state laws; administrative code, and all policies, procedures and regulations related to these systems. FDLE retains full control over the management and operation of CJNet and FCIC.

Therefore, in consideration of the mutual benefits to be derived from this Agreement, the FDLE and the User do hereby agree as follows:

(This User Agreement is designed for use with all Florida criminal justice agencies. If the User does not perform a specific function, the provisions regarding that function will not apply to the User.)

SECTION I FCIC/NCIC/CJNET FDLE REQUIREMENTS

FDLE is duly authorized and agrees to ensure access to the information services provided on CJNet and adhere to the following:

1. Serve as the CSA for the State of Florida and provide the User with access to criminal justice information as is available in the FCIC/NCIC and III systems and NLETS through CJNet, and to serve as the means of exchanging criminal justice information between the User and other criminal justice agencies on CJNet.

2. Provide the opportunity for CJIS certification/re-certification and CJIS Security Awareness training.

3. Provide the User with information concerning privacy and security requirements imposed by state and federal laws, rules and regulations.

4. Provide state criminal history record check services for non-criminal justice purposes as provided by law.

5. Act as the central state repository; provide identification, record keeping, and exchange of Criminal History Record Information (CHRI) services.

6. Facilitate access, using CJNet, to other information applications or systems that the User may be authorized to access.

SECTION II FCIC/NCIC/CJNET USER REQUIREMENTS

By accepting access as set forth above, the User agrees to adhere to the following to ensure continuation of access:

1. USE OF THE SYSTEM: **Use of the CJNet and any system accessed via the CJNet is restricted to the administration of criminal justice or as otherwise specifically authorized or required by statute.** Information obtained from the FCIC/NCIC files, or computer interfaces to other state or federal systems, by means of access granted through CJNet, can only be used for authorized purposes in compliance with FCIC/NCIC and III rules, regulations and operating procedures, and state and federal law. It is the responsibility of the User to insure access to CJNet is for authorized purposes only, and to regulate proper use of the network and information at all times. The User must establish appropriate written standards, which may be incorporated with existing codes of conduct, for disciplining violators of this and any incorporated policy.

   If the User provides an interface between FDLE and other criminal justice agencies it must abide by all of the provisions of this agreement. Agencies that access FDLE systems by interfacing through other agencies must, likewise, abide by all provisions of this agreement. An Interagency User Agreement is required when access to CJNet is provided by the User to another agency.

a. MESSAGES: Only law enforcement and other criminal justice messages shall be sent over and through the CJNet. All messages will be treated as privileged unless otherwise indicated. User should make prudent use of regional and statewide broadcast message requests. All messages must use plain English text in the message.

b. COMPLIANCE: Access FCIC/NCIC and other CJNet applications in strict compliance with applicable CJNet, FCIC, NCIC, III and NLETS policies including, but not limited to, policies, practices and procedures relating to:

i) TIMELINESS: FCIC/NCIC records must be entered, modified, located, cleared, and canceled promptly in order to ensure system accuracy and effectiveness. Users that perform FCIC/NCIC updates for other agencies must comply with timeliness requirements for the records entered for the serviced agencies as well.

ii) HOT FILE ENTRIES: User agencies that have personnel dedicated to maintain a 24-hour, seven-day a week FCIC/NCIC operation will be allowed to make entries into the FCIC/NCIC Hot Files.

(a) Users making entries for another law enforcement agency must execute an Interagency Agreement outlining each agency's responsibilities.

(b) Adult Warrants, Missing Persons and all property records of the FCIC Hot File records, entered by state and local agencies, will be made available to the public on the Internet via the FCIC Public Access System (PAS), unless explicitly flagged by the User for exclusion.

iii) QUALITY ASSURANCE: Appropriate and reasonable quality assurance procedures must be in place, including second party verification during entry, to ensure all entries in FCIC/NCIC are complete, accurate, and valid.

iv) VALIDATION: The User must validate all records that the User has entered into the system for accuracy and retention. To be in compliance with FCIC/NCIC rules, regulations and operating procedures, the User must ensure each record is modified to confirm the successful validation of each record on file in FCIC/NCIC. Failure to modify a record to indicate validation may result in its removal from the file. Users that make entries into the FCIC/NCIC Hot Files are responsible for maintaining written validation procedures.

v) HIT CONFIRMATION: The User must comply with FCIC/NCIC rules, regulations and operating procedures by responding to the hit confirmations in a timely manner (within ten minutes or one-hour depending on priority).

vi) DISSEMINATION: Information obtained from the FCIC/NCIC hot files, CJNet or computer interfaces to other state or federal systems, by means of access granted pursuant to Section 943.0525, F.S., can only be used for official criminal justice purposes.

Compliance with Chapter 119, F.S., is accomplished by directing record requests to FDLE per Chapter 11C-6, F.A.C., and section 943.053(3), F.S. It is the responsibility of the User to ensure that access to the CJNet is for authorized criminal justice purposes only, and to regulate proper access to and use of the network and information at all times.

The User will disseminate CHRI derived from federal records or systems only to criminal justice agencies and only for criminal justice purposes. Criminal justice purposes include criminal justice employment screening.

The User, if functioning in the capacity of a pretrial release program or providing CHRI for a pretrial release program, may disseminate Florida public record information only, in compliance with s. 907.043 (3)(b)7, F.S., which requires "[e]ach pretrial release program [to] prepare a register displaying information that is relevant to the defendants released through such a program." This dissemination shall be restricted to county probation services offices and those criminal justice entities providing the probation offices with information obtained via the FCIC II message switch for the administration of criminal justice.

vii) RETENTION: Criminal history records, whether retrieved from III or the state system, which the User maintains, must be kept in a secure records environment to prevent unauthorized access.

(a) Retention of criminal history records, whether retrieved from III or the state system, for extended periods should only be considered when the time sensitivity of the specific record is important.

(b) When retention of criminal history records, whether retrieved from III or the state system, is no longer required, final disposition will be accomplished in a secure manner in compliance with state law, FCIC/NCIC and III rules, regulations and operating procedures to preclude unauthorized access.

(c) Because CHRI may become outdated at any time, a current criminal history record check should be performed whenever CHRI is used or relied upon by the User. Entry or retention of criminal history records in a separate or local database would be inconsistent with this principle, and is therefore discouraged. The retention of criminal history records, whether retrieved from III or the state system, in a secondary (non-FDLE) database is not authorized by law.

viii) CRIMINAL HISTORY TRANSMISSION: Any electronic device that uses wireless or radio technology to transmit voice data may be used for the transmission of CHRI only when an officer determines there is an immediate need for this information to further an investigation or there is a situation affecting the safety of an officer or the public.

A facsimile machine may be used to transmit criminal history information between criminal justice agencies, provided both agencies have an NCIC Originating Agency Identifier (ORI) and are authorized to receive criminal history information. Appropriate measures must be taken to prevent unauthorized viewing or receipt by unauthorized persons

ix) LOGGING: Each interface agency accessing FCIC/NCIC Hot File and III systems shall ensure that an automated log is maintained. The Hot File portion of this log must be maintained for a minimum of twelve months, and the III portion must be maintained for a minimum of four years.

(a) Automated logging is a feature included in the application software provided by FDLE, and local agencies are encouraged to retain these logs for future reference. Users purchasing or developing an interface to FCIC must ensure logging is an included feature.

(b) The automated transaction log must identify: the operator on all transactions, the agency authorizing all transactions, the requester and secondary recipient for all criminal history transactions. This information can be captured at log-on and can be a name, badge number, serial number, or other unique identifier.

(c) The User may only disseminate information to another authorized recipient and must maintain a record of any dissemination of state or federal criminal history information. This record will reflect at a minimum: (1) date of release; (2) to whom the information relates; (3) to whom the information was released; (4) the State Identification (SID) and/or the FBI number(s); and (5) the purpose

for which the information was requested. The User must also be able to identify the reason for all III inquiries upon request from the FBI or FDLE.

x) INFORMATION ACCESS: The User will allow only properly screened, authorized personnel performing a criminal justice function who have received proper security training to have access to information contained within the CJNet, FCIC/NCIC or other state criminal justice information system files. The User will also provide assistance to other criminal justice agencies not equipped with direct FCIC access in compliance with FCIC/NCIC and III rules, regulations and operating procedures, but only to the extent that such assistance is not otherwise prohibited.

(a) The User will ensure that all personnel who initiate a transaction to the FCIC II message switch are current in CJIS certification.

(b) The User will ensure that persons allowed to complete CJIS certification are at least 18 years of age and are U.S. citizens or have a valid immigration status/visa.

FDLE reserves the right to deny FCIC, CJNet or related programs/ systems access to any individual based on valid, articulable concerns for the security and integrity of FCIC, CJNet or related programs/ systems.

xi) WORKSTATION: FDLE is not responsible for the workstation acquisition, maintenance, operation, repair, supplies or workstation operation personnel costs. The User must notify FDLE immediately, should an FCIC/NCIC workstation malfunction or become inoperable. All costs associated with returning the workstation to operation, other than CJNet costs, will be the User's responsibility. FDLE will assist with executing trouble-shooting procedures.

c. Interface Operations: For systems implemented after December 31, 2008, the User will ensure that all automated interfaces that programmatically (i.e., without human intervention) generate transactions to the FCIC II message switch are restricted to no more than one transaction per second per interface.

2. AUDITS: All agencies having access to CJNet, FCIC/NCIC and the III data shall permit an FDLE appointed inspection team to conduct inquiries with regard to any allegations or potential security violations, as well as for routine audits.

FDLE conducts regularly scheduled compliance and technical security audits of every agency accessing the CJNet to ensure network security, conformity with state law, and compliance with all applicable FDLE, CJNet, FCIC/NCIC and III rules, regulations and operating procedures. Compliance and technical security audits may be conducted at other than regularly scheduled times.

3. TRAINING: The User is responsible for complying with training requirements established in CJIS Security Policy and the rules, regulations, and policies established by FCIC/NCIC, III, FDLE and other CJNet applications. The User is responsible for remaining current in the applications, procedures, and policies and ensuring personnel attend these training sessions.

   a. Only operators who have successfully completed CJIS certification shall be allowed to have unsupervised access to the FCIC/NCIC system.

   b. FCIC/NCIC operators who are in their initial six months of assignment may be permitted supervised access to FCIC/NCIC. Operators must successfully complete CJIS certification within six months of appointment or assignment to duties requiring direct access to FCIC/NCIC.

   c. The User will require all personnel who initiate a transaction to the FCIC II message switch to successfully complete CJIS Certification. The User agrees to remove from FCIC/NCIC access any employee who fails to achieve required certification standards, whose certification has expired, whose certificate is otherwise rescinded or as directed by FDLE.

   d. The User will require all information technology (IT) personnel, including any vendor who will in the course of their official duties initiate a transaction to the FCIC II message switch, to successfully complete CJIS certification.

   e. The User will maintain certification records of all CJIS certified personnel in a current status.

   f. The User will require all IT personnel, including any vendor, responsible for maintaining/supporting any IT component used to process, store or transmit any unencrypted information to or from the FCIC II message switch, to successfully complete the CJIS Online Security Training provided by FDLE.

4. RELOCATION: **Should the User desire to relocate the data circuit(s) and/or equipment connected to CJNet, the User must provide FDLE written notice 90 days in advance of the projected move.** All costs associated with the relocation of the equipment and the data circuit(s), including delays in work order dates, will be borne by User unless FDLE has funding to make changes without charge. The repair and cost of any damages resulting from such relocation will be the User's responsibility.

   The User must also provide 90 days advance notice when requesting additional access to FCIC/CJNet.

5. LIABILITY: The User understands that the FDLE, its officers, and employees shall not be liable in any claim, demand, action, suit, or proceeding, including, but not limited to, any suit in law or in equity, for damages by reason of, or arising out of, any false arrest or imprisonment or for any loss, cost, expense or damages resulting from or arising out of the acts, omissions, or detrimental reliance of the personnel of the User in entering, removing, or relying upon information transmitted through CJNet or in the FCIC/NCIC and NLETS information systems.

6. CRIMINAL HISTORY RECORDS: FDLE is authorized to establish an intrastate automated fingerprint identification system (IAFIS) and an intrastate system for the communication of information relating to crimes, criminals and criminal activity.

   To support the creation and maintenance of the criminal history files, the User, as appropriate, will:

   a. Provide for inclusion in criminal history records information systems, adult and juvenile criminal fingerprints on all felony arrests; adult criminal fingerprints on all misdemeanors and comparable ordinance violation arrests; and juvenile fingerprints on misdemeanor arrests specified at Section 943.051, F.S. The submission of other juvenile misdemeanor arrest fingerprints is optional.

   b. Provide security for CHRI and systems that process or store CHRI, and security training for personnel who receive, handle or have access to CHRI.

   c. Screen all personnel who will have direct access to CHRI and reject for employment personnel who have violated or appear unwilling or incapable of abiding by the requirements outlined in this agreement.

   d. Defer to FDLE on any determination as to what purposes qualify for criminal justice versus non-criminal justice designation, as well as with respect to other purposes that may be authorized by law.

e. Pursuant to a signed interagency agreement as authorized by Florida Statutes and/or federal regulations, the User may share state CHRI. Dissemination of information requires compliance with all applicable statutes, FCIC/NCIC and III rules, regulations and operating procedures, including *logging*. Agencies must maintain confidentiality of such record information that is otherwise exempt from *Section* 119.07(1), F.S., as provided by law.

f. Provide security and establish policies to prevent unauthorized access to or dissemination of sealed records.

SECTION III SECURITY REQUIREMENTS

The User must ensure compliance with the FBI CJIS Security Policy and the rules, regulations, policies and procedures established for CJNet, FCIC/NCIC, III and NLETS, which include but are not limited to System Security, Personnel Security, Physical Security, User Authorization, Technical Security, Dissemination of Information Obtained from the Systems, and Destruction of Records. By accepting access as set forth above, the User agrees to adhere to the following security policies in order to ensure continuation of that access:

1. PERSONNEL BACKGROUND SCREENING and POLICY FOR DISCIPLINE: The User is required to conduct a background investigation on all personnel who are authorized to access FCIC/NCIC/III/CJNet data or systems, IT personnel who maintain/support information technology components used to process, transmit or store unencrypted data to and/or from the FCIC II message switch, and other personnel accessing workstation areas that are unescorted by authorized personnel.

   Good management practices dictate the investigation should be completed prior to employment, but it must, at a minimum, be conducted within the first thirty (30) days of employment or assignment. The User may conduct a preliminary on-line criminal justice employment check.

   Before the background is completed the following requirements must be met:

   a. The User must submit applicant fingerprints for positive comparison against the state and national criminal history and for searching of the Hot Files.

   b. If a record of any kind is found, the User will not permit the operator to have access to the FCIC/NCIC system nor access workstation areas. The User will formally notify the FDLE CJIS Systems Officer (CSO) indicating access will be delayed pending review of the criminal history.

   c. When identification of the applicant has been established by fingerprint comparison and the applicant appears to be a fugitive, have pending criminal charges; have an arrest history for a felony or serious misdemeanor; have been found guilty of, regardless of adjudication, or entered a plea of nolo contendere or guilty to any felony or serious misdemeanor; or to be under the

supervision of the court, the User will refer the matter to the FDLE CSO for review.

d. Applicants who have been found guilty of, regardless of adjudication, or entered a plea of nolo contendere or guilty to a felony, will generally be denied access to FCIC/NCIC. For applicants who have been adjudicated guilty of or have had adjudication withheld on a misdemeanor, the User will notify the CSO of the misdemeanor(s) and acknowledge an intent to permit FCIC/CJNet access. Access will also generally be denied to any person under court supervision for a criminal offense or against whom criminal charges are pending. If a determination is made by FDLE that FCIC/NCIC access by the applicant would not be in the public interest, such access will be denied and the User will be notified in writing of the access denial.

e. Once the original background screening has been completed, if the User learns that a CJIS certified employee has a criminal history or pending charge(s), the User will first determine if the pending charge(s) or record(s) adversely affect(s) the employee's continued employment/access/status with the User. If the employee is placed on leave, terminated or denied access to FCIC by the User, as a result of any pending or unresolved charge(s), the User will notify the CSO of the action taken. Generally, denial of access, pending satisfactory resolution of any such charge(s), and notification to the CSO of that action, will be deemed sufficient corrective action by the User.

   If the User determines that no action is required while the charge(s) are pending or unresolved; i.e., that the employee will continue to be allowed access to FCIC, the User will notify the CSO and explain its rationale for continued access. FDLE reserves the right, as CSA, to deny access to FCIC and associated databases until any such charge(s) are resolved or the situation is clarified.

f. The User will have a written policy for discipline of personnel who access CJNet for purposes that are not authorized, disclose information to unauthorized individuals, or violate FCIC/NCIC or III rules, regulations or operating procedures.

2. PHYSICAL SECURITY: The User will determine the perimeter for the physical security of devices that access or provide access to CJNet. Access shall be limited as to allow completion of required duties. The User must have a written policy that ensures and implements security measures, secures devices that access FCIC/NCIC/CJNet and prevents unauthorized use or viewing of information on these devices. The use of screen blanking software with password protection is recommended for devices that access FCIC/NCIC when the operator may leave the computer unsupervised. FDLE reserves the right to object to equipment location, security measures, qualifications and number of personnel who will be accessing FCIC/NCIC and to suspend or withhold service until such matters are corrected to its reasonable satisfaction.

3. ADMINISTRATIVE SECURITY: The User must designate individual agency contacts to assist the User and FDLE with the information services covered by this agreement. Training for these positions is provided by FDLE, and the User must ensure that its designee is keenly aware of the duties and responsibilities of each respective position. The User is required to provide FDLE with up-to-date contact information.

   a. TERMINAL AGENCY COORDINATOR: Agencies accessing the FCIC/NCIC system must designate a Terminal Agency Coordinator (TAC) to ensure compliance with FCIC/NCIC and III rules, regulations and operating procedures, and to facilitate communication between FDLE and the User. The TAC must maintain a current CJIS Certification. TACs appointed after February 2005 must attend TAC training within six (6) months of being assigned to the position.

   b. INFORMATION SECURITY OFFICER: Agencies accessing the FCIC/NCIC system and/or the CJNet, must designate an Information Security Officer (ISO) to ensure security of the FCIC/NCIC workstations, the connection to CJNet, and any access to the information services provided on CJNet to or by the User.

   c. CJNet POINT OF CONTACT: Agencies accessing applications using Public Key Infrastructure (PKI) security certificates on CJNet must designate a Point of Contact (POC). The POC will receive and approve the issuance and revocation of PKI certificates for the User's members.

   d. FCIC PUBLIC ACCESS SYSTEM (PAS) CONTACT: Agencies making entries into the FCIC Hot Files must designate a PAS Contact. The PAS Contact is responsible for any follow-up activities deemed appropriate by the User in response to tips resulting from the posting of records on the PAS.

   FDLE reserves the right to object to the Users appointment of a TAC, LAI, CJNet Point of Contact or ISO based on valid, articulable concerns for the security and integrity of FCIC, CJNet or related programs/systems.

4. TECHNICAL SECURITY

   a. Dial-up services to FCIC/NCIC and CJNet will be permitted provided the User establishes appropriate security measures to ensure compliance with all rules, regulations, procedures, and the FBI CJIS Security Policy.

   b. All FCIC/NCIC/III data transmitted over any public network segment must be encrypted as required by the FBI CJIS Security Policy. This requirement also applies to any private data circuit that is shared with non-criminal justice users and/or is not under the direct security control of a criminal justice agency.

c. The User must maintain, in current status, and provide upon request by FDLE a complete topological drawing, which depicts the User's network configuration as connected to CJNet. This documentation must clearly indicate all network connections, service agencies and interfaces to other information systems.

d. The User will ensure only authorized criminal justice agencies or agencies authorized by FDLE are permitted access to the CJNet via the User's CJNet connection.

e. The User must ensure all devices with connectivity to CJNet employ virus protection software and such software shall be maintained in accordance with the software vendor's published updates.

f. FCIC and CJNet may only be accessed via computers or interface devices owned by the User or contracted entity. Vendors under contract with the User may be allowed access provided all requirements of the DOJ Security Addendum are complied with and member security training is current.

g. The User will ensure that CJNet-only devices have a Windows or network type password to prevent unauthorized access.

h. To ensure appropriate security precautions are in place, and upon approval from the FDLE Network Administration staff, the User may employ wireless network connectivity (for example the 802.11 wireless networking protocol).

5. COMPUTER SECURITY INCIDENT RESPONSE CAPABILITY: The User must have a written policy documenting the actions to be taken in response to a possible computer security incident. The policy should include identifying, reporting, investigating and recovery from computer security incidents. The User will immediately notify FDLE of any suspected compromise of the CJNet.

6. PENETRATION TESTING: The User shall allow the FBI and/or FDLE to periodically test the ability to penetrate the CJNet through the external network connection or system.

7. SECURITY AUTHORITY: All policies, procedures and operating instructions contained in the FBI CJIS Security Policy and FCIC/NCIC, III and NLETS documents, operating manuals and technical memoranda, are hereby incorporated into and made a part of this agreement, except to the extent that they are inconsistent herewith or legally superseded by higher authority.

8. CLIENT SOFTWARE LICENSE: The FCIC II Client Software (eAgent) license from Diverse Computing, Incorporated is located in the Help menu of the eAgent client software. The FCIC II Client Software (eAgent) license is made a part of and incorporated by reference into this User Agreement and shall be binding on the User upon acceptance of the software.

9. PRIVATE VENDORS: Private vendors which, under contract with the User, are permitted access to information systems that process FCIC/NCIC/III data, shall abide by all aspects of the FBI CJIS Security Addendum. The contract between the User and the vendor will incorporate the Security Addendum to ensure adequate security of FCIC/NCIC/III data. The User will maintain the Security Addendum Certification form for each member of the vendor staff with access to information systems that process FCIC/NCIC/III data. Private vendors permitted such access should be aware of the provisions of s. 817.5681, regarding breach of security of personal information.

10. PASSWORDS: The User will ensure that all personnel who initiate a transaction to the FCIC II message switch have a separate and distinct password for the software/interface used to initiate the transaction. The User will ensure that all interfaces with the FCIC II message switch, operated by the User, follow the password requirements as outlined in the FBI CJIS Security Policy.

11. INDIVIDUAL USER ACCESS: The User will deactivate individual user access to eAgent and/or other FCIC interfaces, other CJNet applications, and FBI Law Enforcement On-line (LEO), upon separation, reassignment or termination of duties, provide individual user access is no longer required for the administration of criminal justice.

SECTION IV MISCELLANEOUS REQUIREMENTS

1. FDLE has received funding from the United States Department of Justice and is subject to and must demand intrastate users of its criminal history record services adhere to US Code (28 U.S.C. section 534), State Statute (Chapter 943 F.S.), Code of Federal Regulations (28 C.F.R. Part 20), Florida Administrative Code (Chapter 11C-6, F.A.C.), FCIC/NCIC and III rules, regulations and operating procedures which this agreement incorporates both present and future.

2. PENALTIES AND LIABILITIES: Any non-compliance with the terms of this Agreement concerning the use and dissemination of criminal history information may subject the User's officers or employees to a fine not to exceed $11,000 as provided for in the Code of Federal Regulations, Title 28, Section 20.25, and/or discontinuance of service. Moreover, certain offenses against system security and the information contained therein are crimes under Florida Statutes and can result in criminal prosecution.

3. PROVISIONS INCORPORATED: The User shall be bound by applicable federal and state laws, federal regulations and the rules of FDLE to the same extent that the User would be if such provisions were fully set out herein. Moreover, this Agreement incorporates both present and future law, regulations and rules.

4. TERMINATION: Either party may terminate this Agreement, with or without cause, upon providing advanced written notice of 45 days. Termination for cause includes, but is not limited to, any change in the law that affects either party's

ability to substantially perform as originally provided in this Agreement. Should the aforementioned circumstances arise, either party may terminate or modify the Agreement accordingly.

FDLE reserves the right to terminate service, without notice, upon presentation of reasonable and credible evidence that the User is violating this Agreement or any pertinent federal or state law, regulation or rule.

5. MODIFICATIONS: Modifications to the provisions in this Agreement shall be valid only through execution of a formal Agreement amendment.

6. ACCOUNTABILITY: To the extent provided by the laws of Florida, the User agrees to be responsible for the negligent acts or omissions of its personnel arising out of or involving any information contained in, received from, entered into or through CJNet, FCIC/NCIC, III and NLETS.

7. ACKNOWLEDGEMENT: The User hereby acknowledges the duties and responsibilities as set out in this Agreement. The User acknowledges that these duties and responsibilities have been developed and approved by FDLE to ensure the reliability, confidentiality, completeness, and accuracy of all records contained in or obtained by means of the CJNet, including the FCIC/NCIC System. The User further acknowledges that failure to comply with these duties and responsibilities will subject its access to various sanctions as approved by the FBI Criminal Justice Information Services Advisory Policy Board. These sanctions may include termination of NCIC services to the User. The User may appeal these sanctions through the CSA.

8. TERM OF AGREEMENT: This agreement will remain in force until it is determined by FDLE that a new agreement is required. The User should initiate the execution of a new agreement when a change of agency chief executive occurs.

IN WITNESS THEREOF, the parties hereto have caused this agreement to be executed by the proper officers and officials.

NAME OF USER AGENCY BROWARD SHERIFF'S OFFICE

AGENCY HEAD

AL LAMBERTI **TITLE** SHERIFF
(PLEASE PRINT)

(SIGNATURE)

DATE 1-15-10

WITNESS Susan Page

Approved as to form and legal sufficiency subject to the execution by the parties

By:
Judith Levine, General Counsel
Office of the General Counsel

Date: 1-15-10

FLORIDA DEPARTMENT OF LAW ENFORCEMENT

BY Donna M. Uzzell **TITLE** Director
(PLEASE PRINT)

(SIGNATURE)

DATE 01/26/10

WITNESS **TITLE** Administrative Asst. II

U. S. Department of Justice
Federal Bureau of Investigation
Criminal Justice Information Services Division

Criminal Justice Information Services (CJIS) Security Policy

Version 5.1
7/13/2012

CJISD-ITS-DOC-08140-5.1

Prepared by:
CJIS Information Security Officer

Approved by:
CJIS Advisory Policy Board

EXECUTIVE SUMMARY

Law enforcement needs timely and secure access to services that provide data wherever and whenever for stopping and reducing crime. In response to these needs, the Advisory Policy Board (APB) recommended to the Federal Bureau of Investigation (FBI) that the Criminal Justice Information Services (CJIS) Division authorize the expansion of the existing security management structure in 1998. Administered through a shared management philosophy, the CJIS Security Policy contains information security requirements, guidelines, and agreements reflecting the will of law enforcement and criminal justice agencies for protecting the sources, transmission, storage, and generation of Criminal Justice Information (CJI). The Federal Information Security Management Act of 2002 provides further legal basis for the APB approved management, operational, and technical security requirements mandated to protect CJI and by extension the hardware, software and infrastructure required to enable the services provided by the criminal justice community.

The essential premise of the CJIS Security Policy is to provide appropriate controls to protect the full lifecycle of CJI, whether at rest or in transit. The CJIS Security Policy provides guidance for the creation, viewing, modification, transmission, dissemination, storage, and destruction of CJI data. This policy applies to every individual—contractor, private entity, noncriminal justice agency representative, or member of a criminal justice entity—with access to, or who operate in support of, criminal justice services and information.

The CJIS Security Policy integrates presidential directives, federal laws, FBI directives and the criminal justice community's APB decisions along with nationally recognized guidance from the National Institute of Standards and Technology. The Policy is presented at both strategic and tactical levels and is periodically updated to reflect the security requirements of evolving business models. The Policy features modular sections enabling more frequent updates to address emerging threats and new security measures. The provided security criteria assists agencies with designing and implementing systems to meet a uniform level of risk and security protection while enabling agencies the latitude to institute more stringent security requirements and controls based on their business model and local needs.

The CJIS Security Policy strengthens the partnership between the FBI and CJIS Systems Agencies (CSA), including, in those states with separate authorities, the State Identification Bureaus. Further, as use of criminal history record information for noncriminal justice purposes continues to expand, the CJIS Security Policy becomes increasingly important in guiding the National Crime Prevention and Privacy Compact Council and State Compact Officers in the secure exchange of criminal justice records.

The policy describes the vision and captures the security concepts that set the policies, protections, roles, and responsibilities with minimal impact from changes in technology. The policy empowers CSAs with the insight and ability to tune their security programs according to their needs, budgets, and resource constraints while remaining compliant with the baseline level of security set forth in this Policy. The CJIS Security Policy provides a secure framework of laws, standards, and elements of published and vetted policies for accomplishing the mission across the broad spectrum of the criminal justice and noncriminal justice communities.

APPROVALS

FBI CJIS	Signature and Date
Mr. George A. White, FBI CJIS Information Security Officer	12/1/10
Mr. Jean W. Archambault, Chief, Technical Planning and Control Unit	
Mr. William G. McKinsey, Chief, Information Technology Management Section	12/1/10
Mr. Jerome M. Pender, Deputy Assistant Director, FBI CJIS Division	12/1/10
Mr. Daniel D. Roberts, Assistant Director, FBI CJIS Division	12/7/20

CJIS Advisory Policy Board	Signature and Date
Captain Charles E. Bush, Vice-Chair, Security and Access Subcommittee	
Captain William M. Tatun, Chair, Security and Access Subcommittee	
Captain Thomas W. Turner, Second Vice-Chair, Advisory Policy Board	
Mr. William Casey, First Vice Chair, Advisory Policy Board	
Colonel Steven F. Cumoletti, Chairman, Advisory Policy Board	

CHANGE MANAGEMENT

Revision	Change Description	Created/Changed by	Date	Approved By
5.0	Policy Rewrite	Security Policy Working Group	02/09/2011	See Signature Page
5.1	Incorporate Calendar Year 2011 APB approved changes and administrative changes	CJIS ISO Program Office	07/13/2012	APB & Compact Council

SUMMARY OF CHANGES

Version 5.1

1. In section 3.2.2(2)e, add "(LASO)"
2. In section 3.2.6, change the words "is to" to the word "shall"
3. Change title of Section 4 to "CRIMINAL JUSTICE INFORMATION AND PERSONALLY IDENTIFIABLE INFORMATION"
4. Rewrite Section 4.2, clarify handling of CHRI and rename "hot files" to "Non-Restricted Files Information"
5. Renumber the following sections:
    a. Section 4.2.3 to section 4.2.4
    b. Section 4.2.4 to section 4.2.5
    c. Section 4.2.4.1 to section 4.2.5.1
    d. Section 4.2.4.2 to section 4.2.5.2
6. In Section 4.2.5.2, change the word "hot" to the words "NCIC Non-restricted"
7. Change "is prohibited" to "shall not be used" in Section 5.5.6.2
8. Remove list item number 2 from Section 5.9.1.8
9. Replace Section 5.10.1.4, Voice over Internet Protocol
10. In section 5.10.4.4, change the word "computer" to the words "user device"
11. In section 5.10.4.4 bullet #2, change the acronym "PC" to the words "user device"
12. Add language to Section 5.12.1.1(1), add requirement for state and national check
13. Add language to Section 5.12.1.2(1), add requirement for state and national check
14. Add definition of "Digital Signature" to Appendix A Terms and Definitions
15. Add definition of "Escort" to Appendix A Terms and Definitions
16. Add definition of "Internet Protocol (IP)" to Appendix A Terms and Definitions
17. Add definition of "Logical Access" to Appendix A Terms and Definitions
18. Add definition of "Physical Access" to Appendix A Terms and Definitions
19. In Appendix A, Social Engineering definition, change the word "manipulation" to the word "manipulating"
20. Add definition of "State of Residency" to Appendix A Terms and Definitions
21. Add definition of "Voice over Internet Protocol (VoIP)" to Appendix A Terms and Definitions
22. Add these acronyms to Appendix B: PSTN, PBX, QoS
23. Remove Appendix C-1.E and reference(s) to that diagram
24. Change Assistant Director signature block, Appendix D-1, CJIS User Agreement
25. Change Assistant Director signature block, Appendix D-3, Noncriminal Justice Agency Agreement & Memorandum of Understanding
26. Change Assistant Director signature block, Appendix D-4, Interagency Connection Agreement
27. Change Appendix F, IT Security Incident Response Form, "Copies To:" block
28. Change the title of Appendix G from "Virtualization" to "Best Practices"
29. Rename Appendix G to Appendix G.1 "Virtualization"
30. Add Appendix G.2 "Voice over Internet Protocol White Paper"
31. Add language to Appendix H, Security Addendum Section 2.01
32. Add reference to Appendix I

TABLE OF CONTENTS

Executive Summary ..... **i**
Approvals ..... **ii**
Change Management ..... **iii**
Summary of Changes ..... **iv**
Table of Contents ..... **v**
List of Figures ..... **x**
1 Introduction **1**
1.1 Purpose 1
1.2 Scope 1
1.3 Relationship to Local Security Policy and Other Policies 1
1.4 Terminology Used in This Document 2
1.5 Distribution of the CJIS Security Policy 2
2 CJIS Security Policy Approach **3**
2.1 CJIS Security Policy Vision Statement 3
2.2 Architecture Independent 3
2.3 Risk Versus Realism 3
3 Roles and Responsibilities **4**
3.1 Shared Management Philosophy 4
3.2 Roles and Responsibilities for Agencies and Parties 4
3.2.1 CJIS Systems Agencies (CSA) 5
3.2.2 CJIS Systems Officer (CSO) 5
3.2.3 Terminal Agency Coordinator (TAC) 6
3.2.4 Criminal Justice Agency (CJA) 6
3.2.5 Noncriminal Justice Agency (NCJA) 6
3.2.6 Contracting Government Agency (CGA) 7
3.2.7 Agency Coordinator (AC) 7
3.2.8 CJIS System Agency Information Security Officer (CSA ISO) 7
3.2.9 Local Agency Security Officer (LASO) 8
3.2.10 FBI CJIS Division Information Security Officer (FBI CJIS ISO) 8
3.2.11 Repository Manager 9
3.2.12 Compact Officer 9
4 Criminal Justice Information and Personally Identifiable Information **10**
4.1 Criminal Justice Information (CJI) 10
4.1.1 Criminal History Record Information (CHRI) 10
4.2 Access, Use and Dissemination of Criminal History Record Information (CHRI), NCIC Restricted Files Information, and NCIC Non-Restricted Files Information 10
4.2.1 Proper Access, Use, and Dissemination of CHRI 11
4.2.2 Proper Access, Use, and Dissemination of NCIC Restricted Files Information 11
4.2.3 Proper Access, Use, and Dissemination of NCIC Non-Restricted Files Information 11
4.2.3.1 For Official Purposes 11
4.2.3.2 For Other Authorized Purposes 11
4.2.3.3 CSO Authority in Other Circumstances 12
4.2.4 Storage 12
4.2.5 Justification and Penalties 12

4.2.5.1 Justification 12
4.2.5.2 Penalties 12
4.3 Personally Identifiable Information (PII) 12
5 Policy and Implementation 14
5.1 Policy Area 1: Information Exchange Agreements 15
5.1.1 Information Exchange 15
5.1.1.1 Information Handling 15
5.1.1.2 State and Federal Agency User Agreements 15
5.1.1.3 Criminal Justice Agency User Agreements 16
5.1.1.4 Interagency and Management Control Agreements 16
5.1.1.5 Private Contractor User Agreements and CJIS Security Addendum 16
5.1.1.6 Agency User Agreements 17
5.1.1.7 Security and Management Control Outsourcing Standard 17
5.1.2 Monitoring, Review, and Delivery of Services 18
5.1.2.1 Managing Changes to Service Providers 18
5.1.3 Secondary Dissemination 18
5.1.4 References/Citations/Directives 18
5.2 Policy Area 2: Security Awareness Training 19
5.2.1 Awareness Topics 19
5.2.1.1 All Personnel 19
5.2.1.2 Personnel with Physical and Logical Access 19
5.2.1.3 Personnel with Information Technology Roles 20
5.2.2 Security Training Records 20
5.2.3 References/Citations/Directives 21
5.3 Policy Area 3: Incident Response 22
5.3.1 Reporting Information Security Events 22
5.3.1.1 Reporting Structure and Responsibilities 22
5.3.1.1.1 FBI CJIS Division Responsibilities 22
5.3.1.1.2 CSA ISO Responsibilities 22
5.3.2 Management of Information Security Incidents 23
5.3.2.1 Incident Handling 23
5.3.2.2 Collection of Evidence 23
5.3.3 Incident Response Training 23
5.3.4 Incident Monitoring 23
5.3.5 References/Citations/Directives 24
5.4 Policy Area 4: Auditing and Accountability 25
5.4.1 Auditable Events and Content (Information Systems) 25
5.4.1.1 Events 25
5.4.1.1.1 Content 25
5.4.2 Response to Audit Processing Failures 26
5.4.3 Audit Monitoring, Analysis, and Reporting 26
5.4.4 Time Stamps 26
5.4.5 Protection of Audit Information 26
5.4.6 Audit Record Retention 26

5.4.7 Logging NCIC and III Transactions....26
5.4.8 References/Citations/Directives....27
5.5 Policy Area 5: Access Control....28
5.5.1 Account Management....28
5.5.2 Access Enforcement....28
5.5.2.1 Least Privilege....28
5.5.2.2 System Access Control....29
5.5.2.3 Access Control Criteria....29
5.5.2.4 Access Control Mechanisms....29
5.5.3 Unsuccessful Login Attempts....30
5.5.4 System Use Notification....30
5.5.5 Session Lock....30
5.5.6 Remote Access....31
5.5.6.1 Personally Owned Information Systems....31
5.5.6.2 Publicly Accessible Computers....31
5.5.7 Wireless Access Restrictions....31
5.5.7.1 All 802.11x Wireless Protocols....31
5.5.7.2 Legacy 802.11 Protocols....33
5.5.7.3 Cellular....33
5.5.7.3.1 Cellular Risk Mitigations....33
5.5.7.3.2 Voice Transmissions Over Cellular Devices....34
5.5.7.4 Bluetooth....34
5.5.8 References/Citations/Directives....36
5.6 Policy Area 6: Identification and Authentication....37
5.6.1 Identification Policy and Procedures....37
5.6.1.1 Use of Originating Agency Identifiers in Transactions and Information Exchanges....37
5.6.2 Authentication Policy and Procedures....37
5.6.2.1 Standard Authentication (Password)....38
5.6.2.2 Advanced Authentication....38
5.6.2.2.1 Advanced Authentication Policy and Rationale....38
5.6.2.2.2 Advanced Authentication Decision Tree....39
5.6.3 Identifier and Authenticator Management....41
5.6.3.1 Identifier Management....41
5.6.3.2 Authenticator Management....41
5.6.4 Assertions....42
5.6.5 References/Citations/Directives....42
5.7 Policy Area 7: Configuration Management....45
5.7.1 Access Restrictions for Changes....45
5.7.1.1 Least Functionality....45
5.7.1.2 Network Diagram....45
5.7.2 Security of Configuration Documentation....45
5.7.3 References/Citations/Directives....45
5.8 Policy Area 8: Media Protection....47

5.8.1 Media Storage and Access 47
5.8.2 Media Transport 47
5.8.2.1 Electronic Media in Transit 47
5.8.2.2 Physical Media in Transit 47
5.8.3 Electronic Media Sanitization and Disposal 47
5.8.4 Disposal of Physical Media 47
5.8.5 References/Citations/Directives 48
5.9 Policy Area 9: Physical Protection 49
5.9.1 Physically Secure Location 49
5.9.1.1 Security Perimeter 49
5.9.1.2 Physical Access Authorizations 49
5.9.1.3 Physical Access Control 49
5.9.1.4 Access Control for Transmission Medium 49
5.9.1.5 Access Control for Display Medium 49
5.9.1.6 Monitoring Physical Access 50
5.9.1.7 Visitor Control 50
5.9.1.8 Access Records 50
5.9.1.9 Delivery and Removal 50
5.9.2 Controlled Area 50
5.9.3 References/Citations/Directives 51
5.10 Policy Area 10: System and Communications Protection and Information Integrity 52
5.10.1 Information Flow Enforcement 52
5.10.1.1 Boundary Protection 52
5.10.1.2 Encryption 53
5.10.1.3 Intrusion Detection Tools and Techniques 53
5.10.1.4 Voice over Internet Protocol 53
5.10.2 Facsimile Transmission of CJI 54
5.10.3 Partitioning and Virtualization 54
5.10.3.1 Partitioning 54
5.10.3.2 Virtualization 54
5.10.4 System and Information Integrity Policy and Procedures 55
5.10.4.1 Patch Management 55
5.10.4.2 Malicious Code Protection 55
5.10.4.3 Spam and Spyware Protection 56
5.10.4.4 Personal Firewall 56
5.10.4.5 Security Alerts and Advisories 56
5.10.4.6 Information Input Restrictions 57
5.10.5 References/Citations/Directives 57
5.11 Policy Area 11: Formal Audits 58
5.11.1 Audits by the FBI CJIS Division 58
5.11.1.1 Triennial Compliance Audits by the FBI CJIS Division 58
5.11.1.2 Triennial Security Audits by the FBI CJIS Division 58
5.11.2 Audits by the CSA 58
5.11.3 Special Security Inquiries and Audits 58
5.11.4 References/Citations/Directives 58
5.12 Policy Area 12: Personnel Security 60

5.12.1 Personnel Security Policy and Procedures 60
5.12.1.1 Minimum Screening Requirements for Individuals Requiring Access to CJI: 60
5.12.1.2 Personnel Screening for Contractors and Vendors 61
5.12.2 Personnel Termination 61
5.12.3 Personnel Transfer 62
5.12.4 Personnel Sanctions 62
5.12.5 References/Citations/Directives 62
Appendix A Terms and Definitions A-1
Appendix B Acronyms B-1
Appendix C Network Topology Diagrams C-1
Appendix D Sample Information Exchange Agreements D-1
Appendix E Security Forums and Organizational Entities E-1
Appendix F IT Security Incident Response Form F-1
Appendix G Best practices G-1
Appendix H Security Addendum H-1
Appendix I References I-1
Appendix J Noncriminal Justice Agency Supplemental Guidance J-1
Appendix K Criminal Justice Agency Supplemental Guidance K-1

LIST OF FIGURES

Figure 1 – Overview Diagram of Strategic Functions and Policy Components....4
Figure 2 – Dissemination of restricted and non-restricted NCIC data....13
Figure 3 – Information Exchange Agreements Implemented by a Local Police Department....18
Figure 4 – Security Awareness Training Implemented by a Local Police Department....21
Figure 5 – Incident Response Process Initiated by an Incident in a Local Police Department....24
Figure 6 – Local Police Department's Use of Audit Logs....27
Figure 7 – A Local Police Department's Access Controls....36
Figure 8 – A Local Police Department's Authentication Controls....42
Figure 9 – Authentication Decision for Known Location....43
Figure 10 – Authentication Decision for Unknown Location....44
Figure 11 – A Local Police Department's Configuration Management Controls....46
Figure 12 – A Local Police Department's Media Management Policies....48
Figure 13 – A Local Police Department's Physical Protection Measures....51
Figure 14 – A Local Police Department's Information Systems & Communications Protections 57
Figure 15 – The Audit of a Local Police Department....59
Figure 16 – A Local Police Department's Personnel Security Controls....62

1 INTRODUCTION

This section details the purpose of this document, its scope, relationship to other information security policies, and its distribution constraints.

1.1 Purpose

The CJIS Security Policy provides Criminal Justice Agencies (CJA) and Noncriminal Justice Agencies (NCJA) with a minimum set of security requirements for the access to Federal Bureau of Investigation (FBI) Criminal Justice Information Services (CJIS) Division systems and information and to protect and safeguard Criminal Justice Information (CJI). This minimum standard of security requirements ensures continuity of information protection. The essential premise of the CJIS Security Policy is to provide the appropriate controls to protect CJI, from creation through dissemination; whether at rest or in transit.

The CJIS Security Policy integrates presidential directives, federal laws, FBI directives, the criminal justice community's Advisory Policy Board (APB) decisions along with nationally recognized guidance from the National Institute of Standards and Technology (NIST) and the National Crime Prevention and Privacy Compact Council (Compact Council).

1.2 Scope

At the consent of the advisory process, and taking into consideration federal law and state statutes, the CJIS Security Policy applies to all entities with access to, or who operate in support of, FBI CJIS Division's services and information. The CJIS Security Policy provides minimum security requirements associated with the creation, viewing, modification, transmission, dissemination, storage, or destruction of CJI.

Entities engaged in the interstate exchange of CJI data for noncriminal justice purposes are also governed by the standards and rules promulgated by the Compact Council.

1.3 Relationship to Local Security Policy and Other Policies

The CJIS Security Policy may be used as the sole security policy for the agency. The local agency may complement the CJIS Security Policy with a local policy, or the agency may develop their own stand-alone security policy; however, the CJIS Security Policy shall always be the minimum standard and local policy may augment, or increase the standards, but shall not detract from the CJIS Security Policy standards.

The agency shall develop, disseminate, and maintain formal, documented procedures to facilitate the implementation of the CJIS Security Policy and, where applicable, the local security policy. The policies and procedures shall be consistent with applicable laws, executive orders, directives, policies, regulations, standards, and guidance. Procedures developed for CJIS Security Policy areas can be developed for the security program in general, and for a particular information system, when required.

This document is a compendium of applicable policies in providing guidance on the minimum security controls and requirements needed to access FBI CJIS information and services. These policies include presidential directives, federal laws, FBI directives and the criminal justice community's APB decisions. State, local, and Tribal CJA may implement more stringent

policies and requirements. Appendix I contains the references while Appendix E lists the security forums and organizational entities referenced in this document.

1.4 Terminology Used in This Document

The following terms are used interchangeably throughout this document:

- Agency and Organization: The two terms in this document refer to any entity that submits or receives information, by any means, to/from FBI CJIS systems or services.
- Information and Data: Both terms refer to CJI.
- System, Information System, Service, or named applications like NCIC: all refer to connections to the FBI's criminal justice information repositories and the equipment used to establish said connections.

Appendix A and B provide an extensive list of the terms and acronyms.

1.5 Distribution of the CJIS Security Policy

The CJIS Security Policy, version 5.0 and later, is a publically available document and may be posted and shared without restrictions.

2 CJIS SECURITY POLICY APPROACH

The CJIS Security Policy represents the shared responsibility between FBI CJIS, CJIS Systems Agency (CSA), and the State Identification Bureaus (SIB) of the lawful use and appropriate protection of CJI. The policy provides a baseline of security requirements for current and planned services and sets a minimum standard for new initiatives.

2.1 CJIS Security Policy Vision Statement

The executive summary of this document describes the vision in terms of business needs for confidentiality, integrity, and availability of information. The APB collaborates with the FBI CJIS Division to ensure that the policy remains updated to meet evolving business, technology and security needs.

2.2 Architecture Independent

Due to advancing technology and evolving business models, the FBI CJIS Division is transitioning from legacy stovepipe systems and moving toward a flexible services approach. Systems such as National Crime Information Center (NCIC), National Instant Criminal Background Check System (NICS), and Integrated Automated Fingerprint Identification System (IAFIS) will continue to evolve and may no longer retain their current system platforms, hardware, or program name. However, the data and services provided by these systems will remain stable.

The CJIS Security Policy looks at the data (information), services, and protection controls that apply regardless of the implementation architecture. Architectural independence is not intended to lessen the importance of systems, but provide for the replacement of one technology with another while ensuring the controls required to protect the information remain constant. This objective and conceptual focus on security policy areas provide the guidance and standards while avoiding the impact of the constantly changing landscape of technical innovations. The architectural independence of the policy provides agencies with the flexibility for tuning their information security infrastructure and policies to reflect their own environments.

2.3 Risk Versus Realism

Every “shall” statement contained within the CJIS Security Policy has been scrutinized for risk versus the reality of resource constraints and real-world application. The purpose of the CJIS Security Policy is to establish the minimum security requirements; therefore, individual agencies are encouraged to implement additional controls to address agency specific risks.

3 ROLES AND RESPONSIBILITIES

3.1 Shared Management Philosophy

In the scope of information security, the FBI CJIS Division employs a shared management philosophy with federal, state, local, and tribal law enforcement agencies. Although an advisory policy board for the NCIC has existed since 1969, the Director of the FBI established the CJIS APB in March 1994 to enable appropriate input and recommend policy with respect to CJIS services. Through the APB and its Subcommittees and Working Groups, consideration is given to the needs of the criminal justice and law enforcement community regarding public policy, statutory and privacy aspects, as well as national security relative to CJIS systems and information. The APB represents federal, state, local, and tribal law enforcement and criminal justice agencies throughout the United States, its territories, and Canada.

The FBI has a similar relationship with the Compact Council, which governs the interstate exchange of criminal history records for noncriminal justice purposes. The Compact Council is mandated by federal law to promulgate rules and procedures for the use of the Interstate Identification Index (III) for noncriminal justice purposes. To meet that responsibility, the Compact Council depends on the CJIS Security Policy as the definitive source for standards defining the security and privacy of records exchanged with noncriminal justice practitioners.

3.2 Roles and Responsibilities for Agencies and Parties

It is the responsibility of all agencies covered under this policy to ensure the protection of CJI between the FBI CJIS Division and its user community. The following figure provides an abstract representation of the strategic functions and roles such as governance and operations.

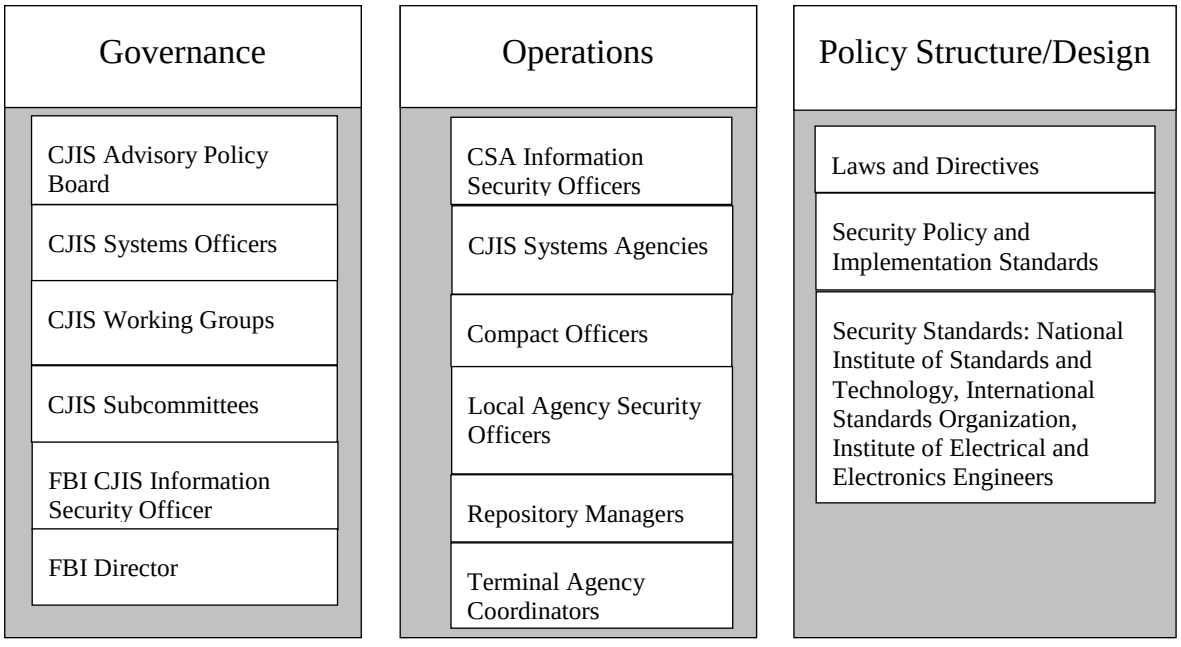


Figure 1 – Overview Diagram of Strategic Functions and Policy Components

This section provides a description of the following entities and roles:

1. CJIS Systems Agency.
2. CJIS Systems Officer.
3. Terminal Agency Coordinator.
4. Criminal Justice Agency.
5. Noncriminal Justice Agency.
6. Contracting Government Agency.
7. Agency Coordinator.
8. CJIS Systems Agency Information Security Officer.
9. Local Agency Security Officer.
10. FBI CJIS Division Information Security Officer.
11. Repository Manager.
12. Compact Officer.

3.2.1 CJIS Systems Agencies (CSA)

The CSA is responsible for establishing and administering an information technology security program throughout the CSA's user community, to include the local levels. The head of each CSA shall appoint a CJIS Systems Officer (CSO). The CSA may impose more stringent protection measures than outlined in this document. Such decisions shall be documented and kept current.

3.2.2 CJIS Systems Officer (CSO)

The CSO is an individual located within the CSA responsible for the administration of the CJIS network for the CSA. Pursuant to the Bylaws for the CJIS Advisory Policy Board and Working Groups, the role of CSO shall not be outsourced. The CSO may delegate responsibilities to subordinate agencies. The CSO shall set, maintain, and enforce the following:

1. Standards for the selection, supervision, and separation of personnel who have access to CJI.
2. Policy governing the operation of computers, access devices, circuits, hubs, routers, firewalls, and other components that comprise and support a telecommunications network and related CJIS systems used to process, store, or transmit CJI, guaranteeing the priority, confidentiality, integrity, and availability of service needed by the criminal justice community.
    a. Ensure appropriate use, enforce system discipline, and ensure CJIS Division operating procedures are followed by all users of the respective services and information.
    b. Ensure state/federal agency compliance with policies approved by the APB and adopted by the FBI.

c. Ensure the appointment of the CSA ISO and determine the extent of authority to the CSA ISO.

d. The CSO, or designee, shall ensure that a Terminal Agency Coordinator (TAC) is designated within each agency that has devices accessing CJIS systems.

e. Ensure each agency having access to CJI has someone designated as the Local Agency Security Officer (LASO).

f. Approve access to FBI CJIS systems.

g. Assume ultimate responsibility for managing the security of CJIS systems within their state and/or agency.

h. Perform other related duties outlined by the user agreements with the FBI CJIS Division.

3. Outsourcing of Criminal Justice Functions

a. Responsibility for the management of the approved security requirements shall remain with the CJA. Security control includes the authority to enforce the standards for the selection, supervision, and separation of personnel who have access to CJI; set and enforce policy governing the operation of computers, circuits, and telecommunications terminals used to process, store, or transmit CJI; and to guarantee the priority service needed by the criminal justice community.

b. Responsibility for the management control of network security shall remain with the CJA. Management control of network security includes the authority to enforce the standards for the selection, supervision, and separation of personnel who have access to CJI; set and enforce policy governing the operation of circuits and network equipment used to transmit CJIS data; and to guarantee the priority service as determined by the criminal justice community.

3.2.3 Terminal Agency Coordinator (TAC)

The TAC serves as the point-of-contact at the local agency for matters relating to CJIS information access. The TAC administers CJIS systems programs within the local agency and oversees the agency's compliance with CJIS systems policies.

3.2.4 Criminal Justice Agency (CJA)

A CJA is defined as a court, a governmental agency, or any subunit of a governmental agency which performs the administration of criminal justice pursuant to a statute or executive order and which allocates a substantial part of its annual budget to the administration of criminal justice. State and federal Inspectors General Offices are included.

3.2.5 Noncriminal Justice Agency (NCJA)

A NCJA is defined (for the purposes of access to CJI) as an entity or any subunit thereof that provides services primarily for purposes other than the administration of criminal justice.

3.2.6 Contracting Government Agency (CGA)

A CGA is a government agency, whether a CJA or a NCJA, that enters into an agreement with a private contractor subject to the CJIS Security Addendum. The CGA entering into an agreement with a contractor shall appoint an agency coordinator.

3.2.7 Agency Coordinator (AC)

An AC is a staff member of the CGA who manages the agreement between the Contractor and agency. The AC shall be responsible for the supervision and integrity of the system, training and continuing education of employees and operators, scheduling of initial training and testing, and certification testing and all required reports by NCIC. The AC shall:

1. Understand the communications, records capabilities, and needs of the Contractor which is accessing federal and state records through or because of its relationship with the CGA.
2. Participate in related meetings and provide input and comments for system improvement.
3. Receive information from the CGA (e.g., system updates) and disseminate it to appropriate Contractor employees.
4. Maintain and update manuals applicable to the effectuation of the agreement, and provide them to the Contractor.
5. Maintain up-to-date records of Contractor's employees who access the system, including name, date of birth, social security number, date fingerprint card(s) submitted, date security clearance issued, and date initially trained, tested, certified or recertified (if applicable).
6. Train or ensure the training of Contractor personnel. If Contractor personnel access NCIC, schedule the operators for testing or a certification exam with the CSA staff, or AC staff with permission from the CSA staff. Schedule new operators for the certification exam within six (6) months of assignment. Schedule certified operators for biennial re-certification testing within thirty (30) days prior to the expiration of certification. Schedule operators for other mandated class.
7. The AC will not permit an untrained/untested or non-certified Contractor employee to access CJI or systems supporting CJI where access to CJI can be gained.
8. Where appropriate, ensure compliance by the Contractor with NCIC validation requirements.
9. Provide completed applicant fingerprint cards on each Contractor employee who accesses the system to the CJA (or, where appropriate, CSA) for criminal background investigation prior to such employee accessing the system.
10. Any other responsibility for the AC promulgated by the FBI.

3.2.8 CJIS System Agency Information Security Officer (CSA ISO)

The CSA ISO shall:

1. Serve as the security point of contact (POC) to the FBI CJIS Division ISO.

2. Document technical compliance with the CJIS Security Policy with the goal to assure the confidentiality, integrity, and availability of criminal justice information to the user community throughout the CSA's user community, to include the local level.
3. Document and provide assistance for implementing the security-related controls for the Interface Agency and its users.
4. Establish a security incident response and reporting procedure to discover, investigate, document, and report to the CSA, the affected criminal justice agency, and the FBI CJIS Division ISO major incidents that significantly endanger the security or integrity of CJI.

3.2.9 Local Agency Security Officer (LASO)

Each LASO shall:

1. Identify who is using the CSA approved hardware, software, and firmware and ensure no unauthorized individuals or processes have access to the same.
2. Identify and document how the equipment is connected to the state system.
3. Ensure that personnel security screening procedures are being followed as stated in this policy.
4. Ensure the approved and appropriate security measures are in place and working as expected.
5. Support policy compliance and ensure the CSA ISO is promptly informed of security incidents.

3.2.10 FBI CJIS Division Information Security Officer (FBI CJIS ISO)

The FBI CJIS ISO shall:

1. Maintain the CJIS Security Policy.
2. Disseminate the FBI Director approved CJIS Security Policy.
3. Serve as a liaison with the CSA's ISO and with other personnel across the CJIS community and in this regard provide technical guidance as to the intent and implementation of operational and technical policy issues.
4. Serve as a point-of-contact (POC) for computer incident notification and distribution of security alerts to the CSOs and ISOs.
5. Assist with developing audit compliance guidelines as well as identifying and reconciling security-related issues.
6. Develop and participate in information security training programs for the CSOs and ISOs, and provide a means by which to acquire feedback to measure the effectiveness and success of such training.
7. Maintain a current ISO homepage on the Law Enforcement Online (LEO) network and keep the CSOs and ISOs updated on pertinent information via the iso@leo.gov email address.

3.2.11 Repository Manager

The State Identification Bureau (SIB) Chief, i.e. Repository Manager, is the designated manager of the agency having oversight responsibility for a state's fingerprint identification services. If both state fingerprint identification services and CJIS systems control are managed within the same state agency, the SIB Chief and CSO may be the same person.

3.2.12 Compact Officer

Pursuant to the National Crime Prevention and Privacy Compact, each party state shall appoint a Compact Officer who shall ensure that Compact provisions and rules, procedures, and standards established by the Compact Council are complied with in their respective state.

4 CRIMINAL JUSTICE INFORMATION AND PERSONALLY IDENTIFIABLE INFORMATION

4.1 Criminal Justice Information (CJI)

Criminal Justice Information is the term used to refer to all of the FBI CJIS provided data necessary for law enforcement and civil agencies to perform their missions including, but not limited to biometric, identity history, biographic, property, and case/incident history data. The following categories of CJI describe the various data sets housed by the FBI CJIS architecture:

1. Biometric Data—data derived from one or more intrinsic physical or behavioral traits of humans typically for the purpose of uniquely identifying individuals from within a population. Used to identify individuals, to include: fingerprints, palm prints, iris scans, and facial recognition data.
2. Identity History Data—textual data that corresponds with an individual's biometric data, providing a history of criminal and/or civil events for the identified individual.
3. Biographic Data—information about individuals associated with a unique case, and not necessarily connected to identity data. Biographic data does not provide a history of an individual, only information related to a unique case.
4. Property Data—information about vehicles and property associated with crime.
5. Case/Incident History—information about the history of criminal incidents.

The intent of the CJIS Security Policy is to ensure the protection of the aforementioned CJI until such time as the information is either released to the public via authorized dissemination (e.g. within a court system or when presented in crime reports data), or is purged or destroyed in accordance with applicable record retention rules.

4.1.1 Criminal History Record Information (CHRI)

Criminal History Record Information (CHRI), sometimes informally referred to as "restricted data", is a subset of CJI. Due to its comparatively sensitive nature, additional controls are required for the access, use and dissemination of CHRI. In addition to the dissemination restrictions outlined below, Title 28, Part 20, Code of Federal Regulations (CFR), defines CHRI and provides the regulatory guidance for dissemination of CHRI. While the CJIS Security Policy attempts to be architecturally independent, the III and the NCIC are specifically identified in Title 28, Part 20, CFR, and the NCIC Operating Manual, as associated with CHRI.

4.2 Access, Use and Dissemination of Criminal History Record Information (CHRI), NCIC Restricted Files Information, and NCIC Non-Restricted Files Information

This section describes the requirements for the access, use and dissemination of CHRI, NCIC restricted files information, and NCIC non-restricted files information.

4.2.1 Proper Access, Use, and Dissemination of CHRI

Information obtained from the III is considered CHRI. Rules governing the access, use, and dissemination of CHRI are found in Title 28, Part 20, CFR. The III shall be accessed only for an authorized purpose. Further, CHRI shall only be used for an authorized purpose consistent with the purpose for which III was accessed. Dissemination to another agency is authorized if (a) the other agency is an Authorized Recipient of such information and is being serviced by the accessing agency, or (b) the other agency is performing personnel and appointment functions for criminal justice employment applicants.

4.2.2 Proper Access, Use, and Dissemination of NCIC Restricted Files Information

The NCIC hosts restricted files and non-restricted files. NCIC restricted files are distinguished from NCIC non-restricted files by the policies governing their access and use. Proper access to, use, and dissemination of data from restricted files shall be consistent with the access, use, and dissemination policies concerning the III described in Title 28, Part 20, CFR, and the NCIC Operating Manual. The restricted files, which shall be protected as CHRI, are as follows:

1. Gang Files.
2. Known or Appropriately Suspected Terrorist Files.
3. Supervised Release Files.
4. Immigration Violator File (formerly the Deported Felon Files).
5. National Sex Offender Registry Files.
6. Historical Protection Order Files of the NCIC.
7. Identity Theft Files.
8. Protective Interest Files.
9. Person With Information (PWI) data in the Missing Person Files.

The remaining NCIC files are considered non-restricted files.

4.2.3 Proper Access, Use, and Dissemination of NCIC Non-Restricted Files Information

4.2.3.1 For Official Purposes

NCIC non-restricted files are those not listed as restricted files in Section 4.2.2. NCIC non-restricted files information may be accessed and used for any authorized purpose consistent with the inquiring agency's responsibility. Information obtained may be disseminated to (a) other government agencies or (b) private entities authorized by law to receive such information for any purpose consistent with their responsibilities.

4.2.3.2 For Other Authorized Purposes

NCIC non-restricted files may be accessed for other purposes consistent with the resources of the inquiring agency; however, requests for bulk data are discouraged. Information derived from NCIC non-restricted files for other than law enforcement purposes can be used by authorized

criminal justice personnel only to confirm the status of a person or property (i.e., wanted or stolen). An inquiring agency is authorized to charge a nominal administrative fee for such service. Non-restricted files information shall not be disseminated commercially.

A response to a NCIC person inquiry may include NCIC restricted files information as well as NCIC non-restricted files information. Agencies shall not disseminate restricted files information for purposes other than law enforcement.

4.2.3.3 CSO Authority in Other Circumstances

If no federal, state or local law or policy prohibition exists, the CSO may exercise discretion to approve or deny dissemination of NCIC non-restricted file information.

4.2.4 Storage

When CHRI is stored, agencies shall establish appropriate administrative, technical and physical safeguards to ensure the security and confidentiality of the information. These records shall be stored for extended periods only when they are key elements for the integrity and/or utility of case files and/or criminal record files. See section 5.9 for physical security controls.

4.2.5 Justification and Penalties

4.2.5.1 Justification

In addition to the use of purpose codes and logging information, all users shall provide a reason for all III inquiries whenever requested by NCIC System Managers, CSAs, local agency administrators, or their representatives.

4.2.5.2 Penalties

Improper access, use or dissemination of CHRI and NCIC Non-Restricted Files information is serious and may result in administrative sanctions including, but not limited to, termination of services and state and federal criminal penalties.

4.3 Personally Identifiable Information (PII)

For the purposes of this document, PII is information which can be used to distinguish or trace an individual's identity, such as name, social security number, or biometric records, alone or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, or mother's maiden name. Any FBI CJIS provided data maintained by an agency, including but not limited to, education, financial transactions, medical history, and criminal or employment history may include PII. A criminal history record for example inherently contains PII as would a Law Enforcement National Data Exchange (N-DEx) case file.

PII shall be extracted from CJI for the purpose of official business only. Agencies shall develop policies, based on state and local privacy rules, to ensure appropriate controls are applied when handling PII extracted from CJI. Due to the expansive nature of PII, this policy does not specify auditing, logging, or personnel security requirements associated with the life cycle of PII.

Figure 2 – Dissemination of restricted and non-restricted NCIC data

A citizen of Springfield went to the Springfield Police Department to request whether his new neighbor, who had been acting suspiciously, had an outstanding warrant. The Springfield Police Department ran an NCIC persons inquiry, which produced a response that included a Wanted Person File (non-restricted file) record and a Known or Appropriately Suspected Terrorist File (restricted file) record. The Springfield Police Department advised the citizen of the outstanding warrant, but did not disclose any information concerning the subject being a known or appropriately suspected terrorist.

5 POLICY AND IMPLEMENTATION

The policy areas focus upon the data and services that the FBI CJIS Division exchanges and provides to the criminal justice community and its partners. Each policy area provides both strategic reasoning and tactical implementation requirements and standards.

While the major theme of the policy areas is concerned with electronic exchange directly with the FBI, it is understood that further dissemination of CJI to Authorized Recipients by various means (hard copy, e-mail, web posting, etc.) constitutes a significant portion of CJI exchanges. Regardless of its form, use, or method of dissemination, CJI requires protection throughout its life.

Not every consumer of FBI CJIS services will encounter all of the policy areas therefore the circumstances of applicability are based on individual agency/entity configurations and usage. Use cases within each of the policy areas will help users relate the policy to their own agency circumstances. The policy areas are:

- Policy Area 1—Information Exchange Agreements
- Policy Area 2—Security Awareness Training
- Policy Area 3—Incident Response
- Policy Area 4—Auditing and Accountability
- Policy Area 5—Access Control
- Policy Area 6—Identification and Authentication
- Policy Area 7—Configuration Management
- Policy Area 8—Media Protection
- Policy Area 9—Physical Protection
- Policy Area 10—Systems and Communications Protection and Information Integrity
- Policy Area 11—Formal Audits
- Policy Area 12—Personnel Security

5.1 Policy Area 1: Information Exchange Agreements

The information shared through communication mediums shall be protected with appropriate security safeguards. The agreements established by entities sharing information across systems and communications mediums are vital to ensuring all parties fully understand and agree to a set of security standards.

5.1.1 Information Exchange

Before exchanging CJI, agencies shall put formal agreements in place that specify security controls. The exchange of information may take several forms including electronic mail, instant messages, web services, facsimile, hard copy, and information systems sending, receiving and storing CJI.

Information exchange agreements outline the roles, responsibilities, and data ownership between agencies and any external parties. Information exchange agreements for agencies sharing CJI data that is sent to and/or received from the FBI CJIS shall specify the security controls and conditions described in this document.

Information exchange agreements shall be supported by documentation committing both parties to the terms of information exchange. As described in subsequent sections, different agreements and policies apply, depending on whether the parties involved are CJAs or NCJAs. See Appendix D for examples of Information Exchange Agreements.

There may be instances, on an ad-hoc basis, where CJI is authorized for further dissemination to Authorized Recipients not covered by an information exchange agreement with the releasing agency. In these instances the dissemination of CJI is considered to be secondary dissemination. See Section 5.1.3 for secondary dissemination guidance.

5.1.1.1 Information Handling

Procedures for handling and storage of information shall be established to protect that information from unauthorized disclosure, alteration or misuse. Using the requirements in this policy as a starting point, the procedures shall apply to the handling, processing, storing, and communication of CJI. These procedures apply to the exchange of CJI no matter the form of exchange.

The policies for information handling and protection also apply to using CJI shared with or received from FBI CJIS for noncriminal justice purposes. In general, a noncriminal justice purpose includes the use of criminal history records for purposes authorized by federal or state law other than purposes relating to the administration of criminal justice, including – but not limited to - employment suitability, licensing determinations, immigration and naturalization matters, and national security clearances.

5.1.1.2 State and Federal Agency User Agreements

Each CSA head or SIB Chief shall execute a signed written user agreement with the FBI CJIS Division stating their willingness to demonstrate conformity with this policy before accessing and participating in CJIS records information programs. This agreement shall include the standards and sanctions governing utilization of CJIS systems. As coordinated through the particular CSA or SIB Chief, each Interface Agency shall also allow the FBI to periodically test

the ability to penetrate the FBI's network through the external network connection or system per authorization of Department of Justice (DOJ) Order 2640.2F. All user agreements with the FBI CJIS Division shall be coordinated with the CSA head.

5.1.1.3 Criminal Justice Agency User Agreements

Any CJA receiving access to FBI CJIS data shall enter into a signed written agreement with the appropriate signatory authority of the CSA providing the access. The written agreement shall specify the FBI CJIS systems and services to which the agency will have access, and the FBI CJIS Division policies to which the agency must adhere. These agreements shall include:

1. Audit.
2. Dissemination.
3. Hit confirmation.
4. Logging.
5. Quality Assurance (QA).
6. Screening (Pre-Employment).
7. Security.
8. Timeliness.
9. Training.
10. Use of the system.
11. Validation.

5.1.1.4 Interagency and Management Control Agreements

A NCJA (government) designated to perform criminal justice functions for a CJA shall be eligible for access to the CJI. Access shall be permitted when such designation is authorized pursuant to executive order, statute, regulation, or inter-agency agreement. The NCJA shall sign and execute a management control agreement (MCA) with the CJA, which stipulates management control of the criminal justice function remains solely with the CJA. The MCA may be a separate document or included with the language of an inter-agency agreement. An example of an NCJA (government) is a city information technology (IT) department.

5.1.1.5 Private Contractor User Agreements and CJIS Security Addendum

The CJIS Security Addendum is a uniform addendum to an agreement between the government agency and a private contractor, approved by the Attorney General of the United States, which specifically authorizes access to CHRI, limits the use of the information to the purposes for which it is provided, ensures the security and confidentiality of the information is consistent with existing regulations and the CJIS Security Policy, provides for sanctions, and contains such other provisions as the Attorney General may require.

Private contractors who perform criminal justice functions shall meet the same training and certification criteria required by governmental agencies performing a similar function, and shall be subject to the same extent of audit review as are local user agencies. All private contractors who perform criminal justice functions shall acknowledge, via signing of the CJIS Security

Addendum Certification page, and abide by all aspects of the CJIS Security Addendum. The CJIS Security Addendum is presented in Appendix H. Modifications to the CJIS Security Addendum shall be enacted only by the FBI.

1. Private contractors designated to perform criminal justice functions for a CJA shall be eligible for access to CJI. Access shall be permitted pursuant to an agreement which specifically identifies the agency's purpose and scope of providing services for the administration of criminal justice. The agreement between the CJA and the private contractor shall incorporate the CJIS Security Addendum approved by the Director of the FBI, acting for the U.S. Attorney General, as referenced in Title 28 CFR 20.33 (a)(7).
2. Private contractors designated to perform criminal justice functions on behalf of a NCJA (government) shall be eligible for access to CJI. Access shall be permitted pursuant to an agreement which specifically identifies the agency's purpose and scope of providing services for the administration of criminal justice. The agreement between the NCJA and the private contractor shall incorporate the CJIS Security Addendum approved by the Director of the FBI, acting for the U.S. Attorney General, as referenced in Title 28 CFR 20.33 (a)(7).

5.1.1.6 Agency User Agreements

A NCJA (public) designated to request civil fingerprint-based background checks, with the full consent of the individual to whom a background check is taking place, for noncriminal justice functions, shall be eligible for access to CJI. Access shall be permitted when such designation is authorized pursuant to federal law or state statute approved by the U.S. Attorney General. An NCJA (public) receiving access to FBI CJIS data shall enter into a signed written agreement with the appropriate signatory authority of the CSA/SIB providing the access. An example of a NCJA (public) is a county school board.

A NCJA (private) designated to request civil fingerprint-based background checks, with the full consent of the individual to whom a background check is taking place, for noncriminal justice functions, shall be eligible for access to CJI. Access shall be permitted when such designation is authorized pursuant to federal law or state statute approved by the U.S. Attorney General. An NCJA (private) receiving access to FBI CJIS data shall enter into a signed written agreement with the appropriate signatory authority of the CSA/SIB providing the access. An example of a NCJA (private) is a local bank.

All NCJAs accessing CJI shall be subject to all pertinent areas of the CJIS Security Policy (see Appendix J for supplemental guidance). Each NCJA that directly accesses FBI CJI shall also allow the FBI to periodically test the ability to penetrate the FBI's network through the external network connection or system per authorization of Department of Justice (DOJ) Order 2640.2F.

5.1.1.7 Security and Management Control Outsourcing Standard

Channelers designated to request civil fingerprint-based background checks or noncriminal justice ancillary functions on behalf of a NCJA (public) or NCJA (private) for noncriminal justice functions shall be eligible for access to CJI. Access shall be permitted when such designation is authorized pursuant to federal law or state statute approved by the U.S. Attorney General. All Channelers accessing CJI shall be subject to the terms and conditions described in

the Compact Council Security and Management Control Outsourcing Standard. Each Channeler that directly accesses CJI shall also allow the FBI to conduct periodic penetration testing.

Channelers leveraging CJI to perform civil functions on behalf of an Authorized Recipient shall meet the same training and certification criteria required by governmental agencies performing a similar function, and shall be subject to the same extent of audit review as are local user agencies.

5.1.2 Monitoring, Review, and Delivery of Services

As specified in the inter-agency agreements, MCAs, and contractual agreements with private contractors, the services, reports and records provided by the service provider shall be regularly monitored and reviewed. The CJA shall maintain sufficient overall control and visibility into all security aspects to include, but not limited to, identification of vulnerabilities and information security incident reporting/response. The incident reporting/response process used by the service provider shall conform to the incident reporting/response specifications provided in this policy.

5.1.2.1 Managing Changes to Service Providers

Any changes to services provided by a service provider shall be managed by the CJA. This includes provision of services, changes to existing services, and new services. Evaluation of the risks to the agency shall be undertaken based on the criticality of the data, system, and the impact of the change.

5.1.3 Secondary Dissemination

If CHRI is released to another authorized agency, and that agency was not part of the releasing agency's primary information exchange agreement(s), the releasing agency shall log such dissemination.

5.1.4 References/Citations/Directives

Appendix I contains all of the references used in this policy and may contain additional sources that apply to this section.

Figure 3 – Information Exchange Agreements Implemented by a Local Police Department

A local police department executed a Memorandum of Understanding (MOU) for the interface with their state CSA. The local police department also executed an MOU (which included an MCA) with the county information technology (IT) department for the day-to-day operations of their criminal-justice infrastructure. The county IT department, in turn, outsourced operations to a local vendor who signed the CJIS Security Addendum.

5.2 Policy Area 2: Security Awareness Training

Basic security awareness training shall be required within six months of initial assignment, and biennially thereafter, for all personnel who have access to CJI. The CSO/SIB may accept the documentation of the completion of security awareness training from another agency. Accepting such documentation from another agency means that the accepting agency assumes the risk that the training may not meet a particular requirement or process required by federal, state, or local laws.

5.2.1 Awareness Topics

A significant number of topics can be mentioned and briefly discussed in any awareness session or campaign. To help further the development and implementation of individual agency security awareness training programs the following baseline guidance is provided.

5.2.1.1 All Personnel

At a minimum, the following topics shall be addressed as baseline security awareness training for all authorized personnel with access to CJI:

1. Rules that describe responsibilities and expected behavior with regard to CJI usage.
2. Implications of noncompliance.
3. Incident response (Points of contact; Individual actions).
4. Media protection.
5. Visitor control and physical access to spaces—discuss applicable physical security policy and procedures, e.g., challenge strangers, report unusual activity.
6. Protect information subject to confidentiality concerns — hardcopy through destruction.
7. Proper handling and marking of CJI.
8. Threats, vulnerabilities, and risks associated with handling of CJI.
9. Dissemination and destruction.

5.2.1.2 Personnel with Physical and Logical Access

In addition to 5.2.1.1 above, the following topics, at a minimum, shall be addressed as baseline security awareness training for all authorized personnel with both physical and logical access to CJI:

1. Rules that describe responsibilities and expected behavior with regard to information system usage.
2. Password usage and management—including creation, frequency of changes, and protection.
3. Protection from viruses, worms, Trojan horses, and other malicious code.
4. Unknown e-mail/attachments.
5. Web usage—allowed versus prohibited; monitoring of user activity.

6. Spam.
7. Social engineering.
8. Physical Security—increases in risks to systems and data.
9. Media Protection.
10. Handheld device security issues—address both physical and wireless security issues.
11. Use of encryption and the transmission of sensitive/confidential information over the Internet—address agency policy, procedures, and technical contact for assistance.
12. Laptop security—address both physical and information security issues.
13. Personally owned equipment and software—state whether allowed or not (e.g., copyrights).
14. Access control issues—address least privilege and separation of duties.
15. Individual accountability—explain what this means in the agency.
16. Use of acknowledgement statements—passwords, access to systems and data, personal use and gain.
17. Desktop security—discuss use of screensavers, restricting visitors' view of information on screen (mitigating "shoulder surfing"), battery backup devices, allowed access to systems.
18. Protect information subject to confidentiality concerns—in systems, archived, on backup media, and until destroyed.
19. Threats, vulnerabilities, and risks associated with accessing CJIS Service systems and services.

5.2.1.3 Personnel with Information Technology Roles

In addition to 5.2.1.1 and 5.2.1.2 above, the following topics at a minimum shall be addressed as baseline security awareness training for all Information Technology personnel (system administrators, security administrators, network administrators, etc.):

1. Protection from viruses, worms, Trojan horses, and other malicious code—scanning, updating definitions.
2. Data backup and storage—centralized or decentralized approach.
3. Timely application of system patches—part of configuration management.
4. Access control measures.
5. Network infrastructure protection measures.

5.2.2 Security Training Records

Records of individual basic security awareness training and specific information system security training shall be documented, kept current, and maintained by the CSO/SIB/Compact Officer. Maintenance of training records can be delegated to the local level.

5.2.3 References/Citations/Directives

Appendix I contains all of the references used in this policy and may contain additional sources that apply to this section.

Figure 4 – Security Awareness Training Implemented by a Local Police Department

A local police department with a staff of 20 sworn law-enforcement officers and 15 support personnel worked with a vendor to develop role-specific security-awareness training, and required all staff to complete this training upon assignment and every two years thereafter. The local police department scheduled the sworn law-enforcement training to coincide with their NCIC certification training. The vendor maintained the training records for the police department's entire staff, and provided reporting to the department to help it ensure compliance with the CJIS Security Policy.

5.3 Policy Area 3: Incident Response

There has been an increase in the number of accidental or malicious computer attacks against both government and private agencies, regardless of whether the systems are high or low profile. Agencies shall: (i) establish an operational incident handling capability for agency information systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities; (ii) track, document, and report incidents to appropriate agency officials and/or authorities.

ISOs have been identified as the POC on security-related issues for their respective agencies and shall ensure LASOs institute the CSA incident response reporting procedures at the local level. Appendix F contains a sample incident notification letter for use when communicating the details of an incident to the FBI CJIS ISO.

5.3.1 Reporting Information Security Events

The agency shall promptly report incident information to appropriate authorities. Information security events and weaknesses associated with information systems shall be communicated in a manner allowing timely corrective action to be taken. Formal event reporting and escalation procedures shall be in place. Wherever feasible, the agency shall employ automated mechanisms to assist in the reporting of security incidents. All employees, contractors and third party users shall be made aware of the procedures for reporting the different types of event and weakness that might have an impact on the security of agency assets and are required to report any information security events and weaknesses as quickly as possible to the designated point of contact.

5.3.1.1 Reporting Structure and Responsibilities

5.3.1.1.1 FBI CJIS Division Responsibilities

The FBI CJIS Division shall:

1. Manage and maintain the CJIS Division's Computer Security Incident Response Capability (CSIRC).
2. Serve as a central clearinghouse for all reported intrusion incidents, security alerts, bulletins, and other security-related material.
3. Ensure additional resources for all incidents affecting FBI CJIS Division controlled systems as needed.
4. Disseminate prompt advisories of system threats and operating system vulnerabilities to all CSOs and ISOs through the use of the **iso@leo.gov** e-mail account, to include but not limited to: Product Security Bulletins, Virus Bulletins, and Security Clips.
5. Track all reported incidents and/or trends.
6. Monitor the resolution of all incidents.

5.3.1.1.2 CSA ISO Responsibilities

The CSA ISO shall:

1. Assign individuals in each state, federal, and international law enforcement organization to be the primary point of contact for interfacing with the FBI CJIS Division concerning incident handling and response.
2. Identify individuals who are responsible for reporting incidents within their area of responsibility.
3. Collect incident information from those individuals for coordination and sharing among other organizations that may or may not be affected by the incident.
4. Develop, implement, and maintain internal incident response procedures and coordinate those procedures with other organizations that may or may not be affected.
5. Collect and disseminate all incident-related information received from the Department of Justice (DOJ), FBI CJIS Division, and other entities to the appropriate local law enforcement POCs within their area.
6. Act as a single POC for their jurisdictional area for requesting incident response assistance.

5.3.2 Management of Information Security Incidents

A consistent and effective approach shall be applied to the management of information security incidents. Responsibilities and procedures shall be in place to handle information security events and weaknesses effectively once they have been reported.

5.3.2.1 Incident Handling

The agency shall implement an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery. Wherever feasible, the agency shall employ automated mechanisms to support the incident handling process.

Incident-related information can be obtained from a variety of sources including, but not limited to, audit monitoring, network monitoring, physical access monitoring, and user/administrator reports. The agency should incorporate the lessons learned from ongoing incident handling activities into the incident response procedures and implements the procedures accordingly.

5.3.2.2 Collection of Evidence

Where a follow-up action against a person or agency after an information security incident involves legal action (either civil or criminal), evidence shall be collected, retained, and presented to conform to the rules for evidence laid down in the relevant jurisdiction(s).

5.3.3 Incident Response Training

The agency shall ensure general incident response roles responsibilities are included as part of required security awareness training.

5.3.4 Incident Monitoring

The agency shall track and document information system security incidents on an ongoing basis. The CSA ISO shall maintain completed security incident reporting forms until the subsequent

FBI triennial audit or until legal action (if warranted) is complete; whichever time-frame is greater.

5.3.5 References/Citations/Directives

Appendix I contains all of the references used in this policy and may contain additional sources that apply to this section.

Figure 5 – Incident Response Process Initiated by an Incident in a Local Police Department

A state ISO received a notification from a local police department that suspicious network activity from a known botnet was detected on their network. The state ISO began the process of collecting all pertinent information about this incident, e.g. incident date/time, points-of-contact, systems affected, nature of the incident, actions taken, etc. and requested that the local police department confirm that their malware signatures were up to date. The state ISO contacted both the FBI CJIS ISO and state CSO to relay the preliminary details of this incident. The FBI CJIS ISO instructed the involved parties to continue their investigation and to submit an incident response form once all the information had been gathered. The FBI CJIS ISO contacted the lead for the FBI CSIRC to inform them that an incident response form was forthcoming. The state ISO gathered the remainder of the information from the local police department and submitted a completed incident response form to the FBI CJIS ISO who subsequently provided it to the FBI CSIRC. The FBI CSIRC notified the Department of Justice Computer Incident Response Team (DOJCIRT). The state ISO continued to monitor the situation, passing relevant details to the FBI CJIS ISO, ultimately determining that the botnet was eliminated from the local police department's infrastructure. Subsequent investigations determined that the botnet was restricted to the department's administrative infrastructure and thus no CJI was compromised.

5.4 Policy Area 4: Auditing and Accountability

Agencies shall implement audit and accountability controls to increase the probability of authorized users conforming to a prescribed pattern of behavior. Agencies shall carefully assess the inventory of components that compose their information systems to determine which security controls are applicable to the various components.

Auditing controls are typically applied to the components of an information system that provide auditing capability (servers, etc.) and would not necessarily be applied to every user-level workstation within the agency. As technology advances, more powerful and diverse functionality can be found in such devices as personal digital assistants and cellular telephones, which may require the application of security controls in accordance with an agency assessment of risk.

5.4.1 Auditable Events and Content (Information Systems)

The agency's information system shall generate audit records for defined events. These defined events include identifying significant events which need to be audited as relevant to the security of the information system. The agency shall specify which information system components carry out auditing activities. Auditing activity can affect information system performance and this issue must be considered as a separate factor during the acquisition of information systems.

The agency's information system shall produce, at the application and/or operating system level, audit records containing sufficient information to establish what events occurred, the sources of the events, and the outcomes of the events. The agency shall periodically review and update the list of agency-defined auditable events. In the event an agency does not use an automated system, manual recording of activities shall still take place.

5.4.1.1 Events

The following events shall be logged:

1. Successful and unsuccessful system log-on attempts.
2. Successful and unsuccessful attempts to access, create, write, delete or change permission on a user account, file, directory or other system resource.
3. Successful and unsuccessful attempts to change account passwords.
4. Successful and unsuccessful actions by privileged accounts.
5. Successful and unsuccessful attempts for users to access, modify, or destroy the audit log file.

5.4.1.1.1 Content

The following content shall be included with every audited event:

1. Date and time of the event.
2. The component of the information system (e.g., software component, hardware component) where the event occurred.
3. Type of event.

4. User/subject identity.
5. Outcome (success or failure) of the event.

5.4.2 Response to Audit Processing Failures

The agency's information system shall provide alerts to appropriate agency officials in the event of an audit processing failure. Audit processing failures include, for example: software/hardware errors, failures in the audit capturing mechanisms, and audit storage capacity being reached or exceeded.

5.4.3 Audit Monitoring, Analysis, and Reporting

The responsible management official shall designate an individual or position to review/analyze information system audit records for indications of inappropriate or unusual activity, investigate suspicious activity or suspected violations, to report findings to appropriate officials, and to take necessary actions. Audit review/analysis shall be conducted at a minimum once a week. The frequency of review/analysis should be increased when the volume of an agency's processing indicates an elevated need for audit review. The agency shall increase the level of audit monitoring and analysis activity within the information system whenever there is an indication of increased risk to agency operations, agency assets, or individuals based on law enforcement information, intelligence information, or other credible sources of information.

5.4.4 Time Stamps

The agency's information system shall provide time stamps for use in audit record generation. The time stamps shall include the date and time values generated by the internal system clocks in the audit records. The agency shall synchronize internal information system clocks on an annual basis.

5.4.5 Protection of Audit Information

The agency's information system shall protect audit information and audit tools from modification, deletion and unauthorized access.

5.4.6 Audit Record Retention

The agency shall retain audit records for at least 365 days. Once the minimum retention time period has passed, the agency shall continue to retain audit records until it is determined they are no longer needed for administrative, legal, audit, or other operational purposes. This includes, for example, retention and availability of audit records relative to Freedom of Information Act (FOIA) requests, subpoena, and law enforcement actions.

5.4.7 Logging NCIC and III Transactions

A log shall be maintained for a minimum of one (1) year on all NCIC and III transactions. The III portion of the log shall clearly identify both the operator and the authorized receiving agency. III logs shall also clearly identify the requester and the secondary recipient. The identification on the log shall take the form of a unique identifier that shall remain unique to the individual requester and to the secondary recipient throughout the minimum one year retention period.

5.4.8 References/Citations/Directives

Appendix I contains all of the references used in this policy and may contain additional sources that apply to this section.

Figure 6 – Local Police Department's Use of Audit Logs

A state CSO contacted a local police department regarding potentially inappropriate use of CHRI that was retrieved using the local department's ORI. The state CSO requested all relevant information from the police department to reconcile state NCIC and III logs against local police department logs. The police department provided the combination of their CJI processing application's logs with relevant operating system and network infrastructure logs to help verify the identity of the users conducting these queries. The review of these logs substantiated the CSO's suspicion.

5.5 Policy Area 5: Access Control

Access control provides the planning and implementation of mechanisms to restrict reading, writing, processing and transmission of CJIS information and the modification of information systems, applications, services and communication configurations allowing access to CJIS information.

5.5.1 Account Management

The agency shall manage information system accounts, including establishing, activating, modifying, reviewing, disabling, and removing accounts. The agency shall validate information system accounts at least annually and shall document the validation process. The validation and documentation of accounts can be delegated to local agencies.

Account management includes the identification of account types (i.e., individual, group, and system), establishment of conditions for group membership, and assignment of associated authorizations. The agency shall identify authorized users of the information system and specify access rights/privileges. The agency shall grant access to the information system based on:

1. Valid need-to-know/need-to-share that is determined by assigned official duties.
2. Satisfaction of all personnel security criteria.

The agency responsible for account creation shall be notified when:

1. A user's information system usage or need-to-know or need-to-share changes.
2. A user is terminated or transferred or associated accounts are removed, disabled, or otherwise secured.

5.5.2 Access Enforcement

The information system shall enforce assigned authorizations for controlling access to the system and contained information. The information system controls shall restrict access to privileged functions (deployed in hardware, software, and firmware) and security-relevant information to explicitly authorized personnel.

Explicitly authorized personnel include, for example, security administrators, system and network administrators, and other privileged users with access to system control, monitoring, or administration functions (e.g., system administrators, information system security officers, maintainers, system programmers).

Access control policies (e.g., identity-based policies, role-based policies, rule-based policies) and associated access enforcement mechanisms (e.g., access control lists, access control matrices, cryptography) shall be employed by agencies to control access between users (or processes acting on behalf of users) and objects (e.g., devices, files, records, processes, programs, domains) in the information system.

5.5.2.1 Least Privilege

The agency shall approve individual access privileges and shall enforce physical and logical access restrictions associated with changes to the information system; and generate, retain, and review records reflecting all such changes. The agency shall enforce the most restrictive set of

rights/privileges or access needed by users for the performance of specified tasks. The agency shall implement least privilege based on specific duties, operations, or information systems as necessary to mitigate risk to CJI. This limits access to CJI to only authorized personnel with the need and the right to know.

Logs of access privilege changes shall be maintained for a minimum of one year or at least equal to the agency's record retention policy – whichever is greater.

5.5.2.2 System Access Control

Access control mechanisms to enable access to CJI shall be restricted by object (e.g., data set, volumes, files, records) including the ability to read, write, or delete the objects. Access controls shall be in place and operational for all IT systems to:

1. Prevent multiple concurrent active sessions for one user identification, for those applications accessing CJI, unless the agency grants authority based upon operational business needs. Agencies shall document the parameters of the operational business needs for multiple concurrent active sessions.
2. Ensure that only authorized personnel can add, change, or remove component devices, dial-up connections, and remove or alter programs.

5.5.2.3 Access Control Criteria

Agencies shall control access to CJI based on one or more of the following:

1. Job assignment or function (i.e., the role) of the user seeking access.
2. Physical location.
3. Logical location.
4. Network addresses (e.g., users from sites within a given agency may be permitted greater access than those from outside).
5. Time-of-day and day-of-week/month restrictions.

5.5.2.4 Access Control Mechanisms

When setting up access controls, agencies shall use one or more of the following mechanisms:

1. Access Control Lists (ACLs). ACLs are a register of users (including groups, machines, processes) who have been given permission to use a particular object (system resource) and the types of access they have been permitted.
2. Resource Restrictions. Access to specific functions is restricted by never allowing users to request information, functions, or other resources for which they do not have access. Three major types of resource restrictions are: menus, database views, and network devices.
3. Encryption. Encrypted information can only be decrypted, and therefore read, by those possessing the appropriate cryptographic key. While encryption can provide strong access control, it is accompanied by the need for strong key management. If encryption of stored information is employed as an access enforcement mechanism, the

cryptography used is Federal Information Processing Standards (FIPS) 140-2 (as amended) compliant (see section 5.10.1.2 for encryption requirements).

4. Application Level. In addition to controlling access at the information system level, access enforcement mechanisms are employed at the application level to provide increased information security for the agency.

5.5.3 Unsuccessful Login Attempts

Where technically feasible, the system shall enforce a limit of no more than 5 consecutive invalid access attempts by a user (attempting to access CJI or systems with access to CJI). The system shall automatically lock the account/node for a 10 minute time period unless released by an administrator.

5.5.4 System Use Notification

The information system shall display an approved system use notification message, before granting access, informing potential users of various usages and monitoring rules. The system use notification message shall, at a minimum, provide the following information:

1. The user is accessing a restricted information system.
2. System usage may be monitored, recorded, and subject to audit.
3. Unauthorized use of the system is prohibited and may be subject to criminal and/or civil penalties.
4. Use of the system indicates consent to monitoring and recording.

The system use notification message shall provide appropriate privacy and security notices (based on associated privacy and security policies or summaries) and remain on the screen until the user acknowledges the notification and takes explicit actions to log on to the information system.

Privacy and security policies shall be consistent with applicable laws, executive orders, directives, policies, regulations, standards, and guidance. System use notification messages can be implemented in the form of warning banners displayed when individuals log in to the information system. For publicly accessible systems:

(i) the system use information is available and when appropriate, is displayed before granting access;

(ii) any references to monitoring, recording, or auditing are in keeping with privacy accommodations for such systems that generally prohibit those activities; and

(iii) the notice given to public users of the information system includes a description of the authorized uses of the system.

5.5.5 Session Lock

The information system shall prevent further access to the system by initiating a session lock after a maximum of 30 minutes of inactivity, and the session lock remains in effect until the user reestablishes access using appropriate identification and authentication procedures. Users shall directly initiate session lock mechanisms to prevent inadvertent viewing when a device is

unattended. A session lock is not a substitute for logging out of the information system. In the interest of officer safety, devices that are: (1) part of a police vehicle; or (2) used to perform dispatch functions and located within a physically secure location, are exempt from this requirement. Note: an example of a session lock is a screen saver with password.

5.5.6 Remote Access

The agency shall authorize, monitor, and control all methods of remote access to the information system. Remote access is any temporary access to an agency's information system by a user (or an information system) communicating temporarily through an external, non-agency-controlled network (e.g., the Internet).

The agency shall employ automated mechanisms to facilitate the monitoring and control of remote access methods. The agency shall control all remote accesses through managed access control points. The agency may permit remote access for privileged functions only for compelling operational needs but shall document the rationale for such access in the security plan for the information system.

5.5.6.1 Personally Owned Information Systems

A personally owned information system shall not be authorized to access, process, store or transmit CJI unless the agency has established and documented the specific terms and conditions for personally owned information system usage.

This control does not apply to the use of personally owned information systems to access agency's information systems and information that are intended for public access (e.g., an agency's public website that contains purely public information).

5.5.6.2 Publicly Accessible Computers

Publicly accessible computers shall not be used to access, process, store or transmit CJI. Publicly accessible computers include but are not limited to: hotel business center computers, convention center computers, public library computers, public kiosk computers, etc.

5.5.7 Wireless Access Restrictions

The agency shall: (i) establish usage restrictions and implementation guidance for wireless technologies; and (ii) authorize, monitor, control wireless access to the information system. Wireless technologies, in the simplest sense, enable one or more devices to communicate without physical connections—without requiring network or peripheral cabling.

Examples of wireless technologies include, but are not limited to: 802.11x, cellular networks, Bluetooth, satellite and microwave. Wireless technologies require at least the minimum security applied to wired technology and, based upon the specific technology, may require some additional security controls as described below.

5.5.7.1 All 802.11x Wireless Protocols

Agencies shall:

1. Perform validation testing to ensure rogue APs (Access Points) do not exist in the 802.11 Wireless Local Area Network (WLAN) and to fully understand the wireless network security posture.
2. Maintain a complete inventory of all Access Points (APs) and 802.11 wireless devices.
3. Place APs in secured areas to prevent unauthorized physical access and user manipulation.
4. Test AP range boundaries to determine the precise extent of the wireless coverage and design the AP wireless coverage to limit the coverage area to only what is needed for operational purposes.
5. Enable user authentication and encryption mechanisms for the management interface of the AP.
6. Ensure that all APs have strong administrative passwords and ensure that all passwords are changed in accordance with section 5.6.2.1.
7. Ensure the reset function on APs is used only when needed and is only invoked by authorized personnel. Restore the APs to the latest security settings, when the reset functions are used, to ensure the factory default settings are not utilized.
8. Change the default service set identifier (SSID) in the APs. Disable the broadcast SSID feature so that the client SSID must match that of the AP. Validate that the SSID character string does not contain any agency identifiable information (division, department, street, etc.) or services.
9. Enable all security features of the wireless product, including the cryptographic authentication, firewall, and other privacy features.
10. Ensure that encryption key sizes are at least 128-bits and the default shared keys are replaced by unique keys.
11. Ensure that the ad hoc mode has been disabled unless the environment is such that the risk has been assessed and is tolerable. Note: some products do not allow disabling this feature; use with caution or use different vendor.
12. Disable all nonessential management protocols on the APs and disable hypertext transfer protocol (HTTP) when not needed or protect HTTP access with authentication and encryption.
13. Enable logging (if supported) and review the logs on a recurring basis per local policy. At a minimum logs shall be reviewed monthly.
14. Segregate, virtually (e.g. virtual local area network (VLAN) and ACLs) or physically (e.g. firewalls), the wireless network from the operational wired infrastructure. Limit access between wireless networks and the wired network to only operational needs.
15. When disposing of access points that will no longer be used by the agency, clear access point configuration to prevent disclosure of network configuration, keys, passwords, etc.

5.5.7.2 Legacy 802.11 Protocols

Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA) cryptographic algorithms, used by all pre-802.11i protocols, do not meet the requirements for FIPS 140-2 and are to be used only if additional security controls are employed.

Agencies shall follow the guidelines below regarding wireless implementation and cases where the WEP and WPA security features are used to provide wireless security in conjunction with the CJIS required minimum encryption specifications.

1. Deploy media access control (MAC) access control lists (ACL); however, MAC ACLs do not represent a strong defense mechanism by themselves because they are transmitted in the clear from WLAN clients to APs so they can be captured easily.
2. Enable WEP/WPA.
3. Ensure the default shared keys are replaced by more secure unique keys.
4. Enable utilization of key-mapping keys rather than default keys so that sessions are unique when using WEP.

5.5.7.3 Cellular

Cellular telephones, smartphones (i.e. Blackberry, iPhones, etc.), personal digital assistants (PDA), and "aircards" are examples of cellular handheld devices or devices that employ cellular technology. Additionally, cellular handheld devices typically include Bluetooth, infrared, and other wireless protocols capable of joining infrastructure networks or creating dynamic ad hoc networks. Cellular devices are at risk due to a multitude of threats and consequently pose a risk to the enterprise.

Threats to cellular handheld devices stem mainly from their size, portability, and available wireless interfaces and associated services. Examples of threats to cellular handheld devices include:

1. Loss, theft, or disposal.
2. Unauthorized access.
3. Malware.
4. Spam.
5. Electronic eavesdropping.
6. Electronic tracking (threat to security of data and safety of law enforcement officer).
7. Cloning (not as prevalent with later generation cellular technologies).
8. Server-resident data.

5.5.7.3.1 Cellular Risk Mitigations

Organizations shall, at a minimum, ensure that cellular devices:

1. Apply available critical patches and upgrades to the operating system.
2. Are configured for local device authentication.

3. Use advanced authentication.
4. Encrypt all CJI resident on the device.
5. Erase cached information when session is terminated.
6. Employ personal firewalls.
7. Employ antivirus software.

5.5.7.3.2 Voice Transmissions Over Cellular Devices

Any cellular device used to transmit CJI via voice is exempt from the encryption and authentication requirements when an officer determines there is an immediate need for the CJI to further an investigation or situations affecting the safety of an officer or the general public.

5.5.7.4 Bluetooth

Bluetooth is an open standard for short-range radio frequency (RF) communication and is used primarily to establish wireless personal area networks (WPAN), commonly referred to as ad hoc networks or piconets. A piconet is composed of two or more Bluetooth devices in close physical proximity that operate on the same channel using the same frequency hopping sequence and can scale to include up to seven active slave devices and up to 255 inactive slave devices. Bluetooth voice and data transfer technology has been integrated into many types of business and consumer devices, including cellular phones, personal digital assistants (PDA), laptops, automobiles, printers, and headsets.

Bluetooth does not provide end-to-end, audit, or non-repudiation security services. If such services are needed, they shall be provided through additional, higher-layer means in addition to the Bluetooth specification and 802.11 standards.

The cryptographic algorithms employed by the Bluetooth standard are not FIPS approved. When communications require FIPS-approved cryptographic protection, this can be achieved by employing application-level FIPS-approved encryption over the native Bluetooth encryption.

Agencies shall:

1. Provide users with a list of precautionary measures they should take to better protect handheld Bluetooth devices from theft. The organization and its employees should be responsible for its wireless technology components because theft of those components could lead to malicious activities against the organization's information system resource.
2. Maintain a complete inventory of all Bluetooth-enabled wireless devices and addresses (BD_ADDRs). A complete inventory of Bluetooth-enabled wireless devices can be referenced when conducting an audit that searches for unauthorized use of wireless technologies.
3. Change the default setting of the Bluetooth device to reflect the organization's security policy. Because default settings are generally not secure, a careful review of those settings should be performed to ensure that they comply with the organization's security policy.
4. Set Bluetooth devices to the lowest necessary and sufficient power level so that transmissions remain within the secure perimeter of the organization. Setting Bluetooth

devices to the lowest necessary and sufficient power level ensures a secure range of access to authorized users. The use of Class 1 devices should be avoided due to their extended range (approximately 100 meters).

5. Choose personal identification number (PIN) codes that are sufficiently random and long. Avoid static and weak PINs, such as all zeroes. PIN codes should be random so that they cannot be easily reproduced by malicious users. Longer PIN codes are more resistant to brute force attacks. For Bluetooth v2.0 (or earlier) devices, an eight-character alphanumeric PIN shall be used.
6. For v2.1 devices using Secure Simple Pairing, avoid using the "Just Works" model. The "Just Works" model does not provide protection against man-in-the-middle (MITM) attacks. Devices that only support Just Works should not be procured if similarly qualified devices that support one of the association models (i.e. Numeric Comparison, Out of Band, or Passkey Entry) are available.
7. Bluetooth devices should be configured by default as, and remain, undiscoverable except as needed for pairing. Bluetooth interfaces should be configured as non-discoverable, which prevents visibility to other Bluetooth devices except when discovery is specifically needed. Also, the default self-identifying or discoverable names provided on Bluetooth devices should be changed to anonymous unidentifiable names.
8. Invoke link encryption for all Bluetooth connections regardless of how needless encryption may seem (i.e. no Security Mode 1). Link encryption should be used to secure all data transmissions during a Bluetooth connection; otherwise, transmitted data is vulnerable to eavesdropping.
9. If multi-hop wireless communication is being utilized, ensure that encryption is enabled on every link in the communication chain. Every link should be secured because one unsecured link results in compromising the entire communication chain.
10. Ensure device mutual authentication is performed for all accesses. Mutual authentication is required to provide verification that all devices on the network are legitimate.
11. Enable encryption for all broadcast transmission (Encryption Mode 3). Broadcast transmissions secured by link encryption provide a layer of security that protects these transmissions from user interception for malicious purposes.
12. Configure encryption key sizes to the maximum allowable. Using maximum allowable key sizes provides protection from brute force attacks.
13. Establish a "minimum key size" for any negotiation process. Establishing minimum key sizes ensures that all keys are long enough to be resistant to brute force attacks. See Section 5.10.1.2 for minimum key encryption standards.
14. Use Security Mode 3 in order to provide link-level security prior to link establishment.
15. Users do not accept transmissions of any kind from unknown or suspicious devices. These types of transmissions include messages, files, and images. With the increase in the number of Bluetooth enabled devices, it is important that users only establish connections with other trusted devices and only accept content from these trusted devices.

5.5.8 References/Citations/Directives

Appendix I contains all of the references used in this policy and may contain additional sources that apply to this section.

Figure 7 – A Local Police Department's Access Controls

A local police department purchased a new computer-assisted dispatch (CAD) system that integrated with their state CSA's CJI interfaces. In doing so, the police department employed least-privilege practices to ensure that its employees were only given those privileges needed to perform their jobs, and as such, excluding IT administrators, employees had only non-administrative privileges on all equipment they used. The police department also used ACLs in the operating systems to control access to the CAD client's executables. The CAD system used internal role-based access controls to ensure only those users that needed access to CJI were given it. The police department performed annual audits of user accounts on all systems under their control including remote access mechanisms, operating systems, and the CAD system to ensure all accounts were in valid states. The police department implemented authentication-failure account lockouts, system use notification via login banners, and screen-saver passwords on all equipment that processes CJI.

5.6 Policy Area 6: Identification and Authentication

The agency shall identify information system users and processes acting on behalf of users and authenticate the identities of those users or processes as a prerequisite to allowing access to agency information systems or services.

5.6.1 Identification Policy and Procedures

Each person who is authorized to store, process, and/or transmit CJI shall be uniquely identified. A unique identification shall also be required for all persons who administer and maintain the system(s) that access CJI or networks leveraged for CJI transit. The unique identification can take the form of a full name, badge number, serial number, or other unique alphanumeric identifier. Agencies shall require users to identify themselves uniquely before the user is allowed to perform any actions on the system. Agencies shall ensure that all user IDs belong to currently authorized users. Identification data shall be kept current by adding new users and disabling and/or deleting former users.

5.6.1.1 Use of Originating Agency Identifiers in Transactions and Information Exchanges

An FBI authorized originating agency identifier (ORI) shall be used in each transaction on CJIS systems in order to identify the sending agency and to ensure the proper level of access for each transaction. The original identifier between the requesting agency and the CSA/SIB/Channeler shall be the ORI, and other agency identifiers, such as user identification or personal identifier, an access device mnemonic, or the Internet Protocol (IP) address.

Agencies may act as a servicing agency and perform transactions on behalf of authorized agencies requesting the service. Servicing agencies performing inquiry transactions on behalf of another agency may do so using the requesting agency's ORI. Servicing agencies may also use their own ORI to perform inquiry transactions on behalf of a requesting agency if the means and procedures are in place to provide an audit trail for the current specified retention period. Because the agency performing the transaction may not necessarily be the same as the agency requesting the transaction, the CSA/SIB/Channeler shall ensure that the ORI for each transaction can be traced, via audit trail, to the specific agency which is requesting the transaction.

Audit trails can be used to identify the requesting agency if there is a reason to inquire into the details surrounding why an agency ran an inquiry on a subject. Agencies assigned a P (limited access) ORI shall not use the full access ORI of another agency to conduct an inquiry transaction.

5.6.2 Authentication Policy and Procedures

Authentication refers to mechanisms or processes that verify users are valid once they are uniquely identified. The CSA/SIB may develop an authentication strategy which centralizes oversight but decentralizes the establishment and daily administration of the security measures for access to CJI.

Each individual's identity shall be authenticated at either the local agency, CSA, SIB or Channeler level. The authentication strategy shall be part of the agency's audit for policy compliance. The FBI CJIS Division shall identify and authenticate all individuals who establish

direct web-based interactive sessions with FBI CJIS Services. The FBI CJIS Division shall authenticate the ORI of all message-based sessions between the FBI CJIS Division and its customer agencies but will not further authenticate the user nor capture the unique identifier for the originating operator because this function is performed at the local agency, CSA, SIB or Channeler level.

5.6.2.1 Standard Authentication (Password)

Agencies shall follow the secure password attributes, below, to authenticate an individual's unique ID. Passwords shall:

1. Be a minimum length of eight (8) characters on all systems.
2. Not be a dictionary word or proper name.
3. Not be the same as the Userid.
4. Expire within a maximum of 90 calendar days.
5. Not be identical to the previous ten (10) passwords.
6. Not be transmitted in the clear outside the secure location.
7. Not be displayed when entered.

5.6.2.2 Advanced Authentication

Advanced Authentication (AA) provides for additional security to the typical user identification and authentication of login ID and password, such as: biometric systems, user-based public key infrastructure (PKI), smart cards, software tokens, hardware tokens, paper (inert) tokens, or "Risk-based Authentication" that includes a software token element comprised of a number of factors, such as network information, user information, positive device identification (i.e. device forensics, user pattern analysis and user binding), user profiling, and high-risk challenge/response questions.

5.6.2.2.1 Advanced Authentication Policy and Rationale

The requirement to use or not use AA is dependent upon the physical, personnel and technical security controls associated with the user location. For example, AA shall not be required for users requesting access to CJI from within the perimeter of a physically secure location (Section 5.9), when the technical security controls have been met (Sections 5.5 and 5.10). Conversely, if the technical security controls have not been met AA shall be required even if the request for CJI originates from within a physically secure location. Section 5.6.2.2.2 provides agencies with a decision tree to help guide AA decisions.

INTERIM COMPLIANCE:

1. For interim compliance, users accessing CJI from devices associated with, and located within, a police vehicle are exempt from the AA requirement until September 30th 2013 if the information system being used has not been procured or upgraded anytime after September 30th, 2005. For the purposes of this policy, a police vehicle is defined as an enclosed criminal justice conveyance with the capability to comply, during operational periods, with Section 5.9.1.3.

2. Internet Protocol Security (IPSec) does not meet the 2011 requirements for advanced authentication; however, agencies that have funded/implemented IPSec in order to meet the AA requirements of CJIS Security Policy v.4.5 may continue to utilize IPSec for AA until 2013. Examples:

    a. A police officer runs a query for CJI from his/her laptop mounted in a police vehicle. The police officer leverages a cellular network as the transmission medium; authenticates the device using IPSec key exchange; and tunnels across the cellular network using the IPSec virtual private network (VPN). IPSec was funded and installed in order to meet the AA requirements of CJIS Security Policy version 4.5. AA requirements are waived until 2013.

    b. A detective accesses CJI from various locations while investigating a crime scene. The detective uses an agency managed laptop with IPSec installed and leverages a cellular network as the transmission medium. IPSec was funded and installed in order to meet the AA requirements of CJIS Security Policy version 4.5. AA requirements are waived until 2013.

EXCEPTION:

AA shall be required when the requested service has built AA into its processes and requires a user to provide AA before granting access. EXAMPLES:

a. A user, irrespective of his/her location, accesses the LEO website. The LEO has AA built into its services and requires AA prior to granting access. AA is required.

b. A user, irrespective of their location, accesses a State's portal through which access to CJI is facilitated. The State Portal has AA built into its processes and requires AA prior to granting access. AA is required.

5.6.2.2.2 Advanced Authentication Decision Tree

The following AA Decision Tree, coupled with figures 9 and 10 below, assist decision makers in determining whether or not AA is required.

1. Can request's originating location be determined physically?

    If either (a) or (b) below are true the answer to the above question is "yes". Proceed to question 2.

    a. The IP address is attributed to a physical structure; or

    b. The mnemonic is attributed to a specific device assigned to a specific location that is a physical structure.

    If neither (a) or (b) above are true then the answer is "no". Skip to question number 4.

2. Does request originate from within a physically secure location (that is not a police vehicle) as described in section 5.9.1?

    If either (a) or (b) below are true the answer to the above question is "yes". Proceed to question 3.

a. The IP address is attributed to a physically secure location; or

b. If a mnemonic is used it is attributed to a specific device assigned to a specific physically secure location.

If neither (a) or (b) above are true then the answer is "no". Decision tree completed. AA required.

3. Are all required technical controls implemented at this location or at the controlling agency?

   If either (a) or (b) below are true the answer to the above question is "yes". Decision tree completed. AA requirement waived.

   a. Appropriate technical controls listed in sections 5.5 and 5.10 are implemented; or

   b. The controlling agency (i.e. parent agency or agency leveraged as conduit to FBI CJIS data) extends its wide area network controls down to the requesting agency and the extended controls provide assurance equal or greater to the controls listed in sections 5.5 and 5.10.

   If neither (a) or (b) above are true then the answer is "no". Decision tree completed. AA required.

4. Does request originate from an agency-managed user device?

   If either (a) or (b) below are true the answer to the above question is "yes". Proceed to question 5.

   a. The static IP address or MAC address can be traced to registered device; or

   b. Certificates are issued to agency managed devices only and certificate exchange is allowed only between authentication server and agency issued devices.

   If neither (a) or (b) above are true then the answer is "no". Decision tree completed. AA required.

5. Is the agency managed user device associated with a law enforcement conveyance?

   If any of the (a), (b), or (c) statements below is true the answer to the above question is "yes". Proceed to question 6.

   a. The static IP address or MAC address is associated with a device associated with a law enforcement conveyance; or

   b. The certificate presented is associated with a device associated with a law enforcement conveyance; or

   c. The mnemonic presented is associated with a specific device assigned and that device is attributed to a law enforcement conveyance.

   If none of the (a), (b), or (c) statements above are true then the answer is "no". Skip to question number 7.

6. Has there been an acquisition or upgrade since 2005?

   If any of the (a), (b), (c), or (d) statements below are true the answer to the above question is "yes". Proceed to question number 7.

   a. The "green-screen" MDTs have been replaced with laptops or other mobile devices; or

   b. An upgrade of technology exceeding 25% of the cost of the system being upgraded has taken place; or

   c. Any upgrade to the system encryption module has taken place; or

   d. Any upgrade to the system that is not replacing like technology has taken place.

   If none of the (a), (b), (c), or (d) statements above are true then the answer is "no". Decision tree completed. AA requirement waived.

7. Was IPSec implemented to meet the requirements of Policy Version 4.5?

   If either (a) or (b) below are true the answer to the above question is "yes". Decision tree completed. AA requirement is waived.

   a. The budget acquisition of IPSec was completed prior to January 1st, 2009 and IPSec was subsequently implemented; or

   b. Implementation of IPSec was completed prior to January 1st, 2009.

   If neither (a) or (b) above are true then the answer is "no". Decision tree completed. AA required.

5.6.3 Identifier and Authenticator Management

The agency shall establish identifier and authenticator management processes.

5.6.3.1 Identifier Management

In order to manage user identifiers, agencies shall:

1. Uniquely identify each user.
2. Verify the identity of each user.
3. Receive authorization to issue a user identifier from an appropriate agency official.
4. Issue the user identifier to the intended party.
5. Disable the user identifier after a specified period of inactivity.
6. Archive user identifiers.

5.6.3.2 Authenticator Management

In order to manage information system authenticators, agencies shall:

1. Define initial authenticator content.

2. Establish administrative procedures for initial authenticator distribution, for lost/compromised, or damaged authenticators, and for revoking authenticators.
3. Change default authenticators upon information system installation.
4. Change/refresh authenticators periodically.

Information system authenticators include, for example, tokens, user-based PKI certificates, biometrics, passwords, and key cards. Users shall take reasonable measures to safeguard authenticators including maintaining possession of their individual authenticators, not loaning or sharing authenticators with others, and immediately reporting lost or compromised authenticators.

5.6.4 Assertions

Identity providers can be leveraged to identify individuals and assert the individual's identity to a service or to a trusted broker who will in-turn assert the identity to a service. Assertion mechanisms used to communicate the results of a remote authentication to other parties shall be:

1. Digitally signed by a trusted entity (e.g., the identity provider).
2. Obtained directly from a trusted entity (e.g. trusted broker) using a protocol where the trusted entity authenticates to the relying party using a secure protocol (e.g. transport layer security [TLS]) that cryptographically authenticates the verifier and protects the assertion.

Assertions generated by a verifier shall expire after 12 hours and shall not be accepted thereafter by the relying party.

5.6.5 References/Citations/Directives

Appendix C contains all of the references used in this policy and may contain additional sources that apply to this section.

Figure 8 – A Local Police Department's Authentication Controls

During the course of an investigation, a detective accessed CJI from a hotel room using an agency issued mobile broadband card. To gain access, the detective first established the remote session via a secure virtual private network (VPN) tunnel (satisfying the requirement for encryption), then was challenged to enter both password and the value from a hardware token (satisfying the requirement for advanced authentication). Once the detective's credentials were validated, his identity was asserted by the infrastructure to all authorized applications needed to complete his investigation.

Figure 9 – Authentication Decision for Known Location

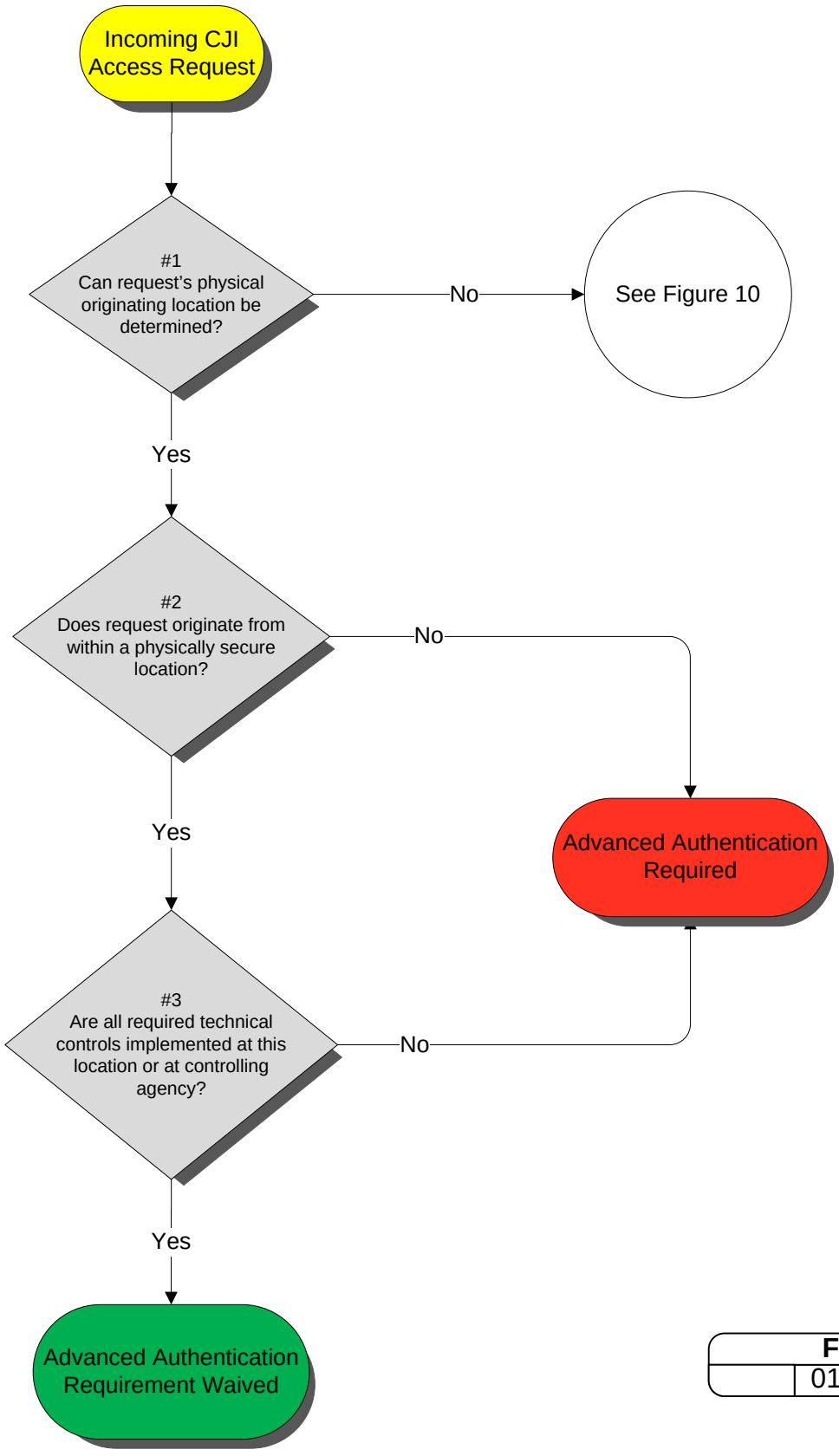


Figure 9
01/01/2011

Figure 10 – Authentication Decision for Unknown Location

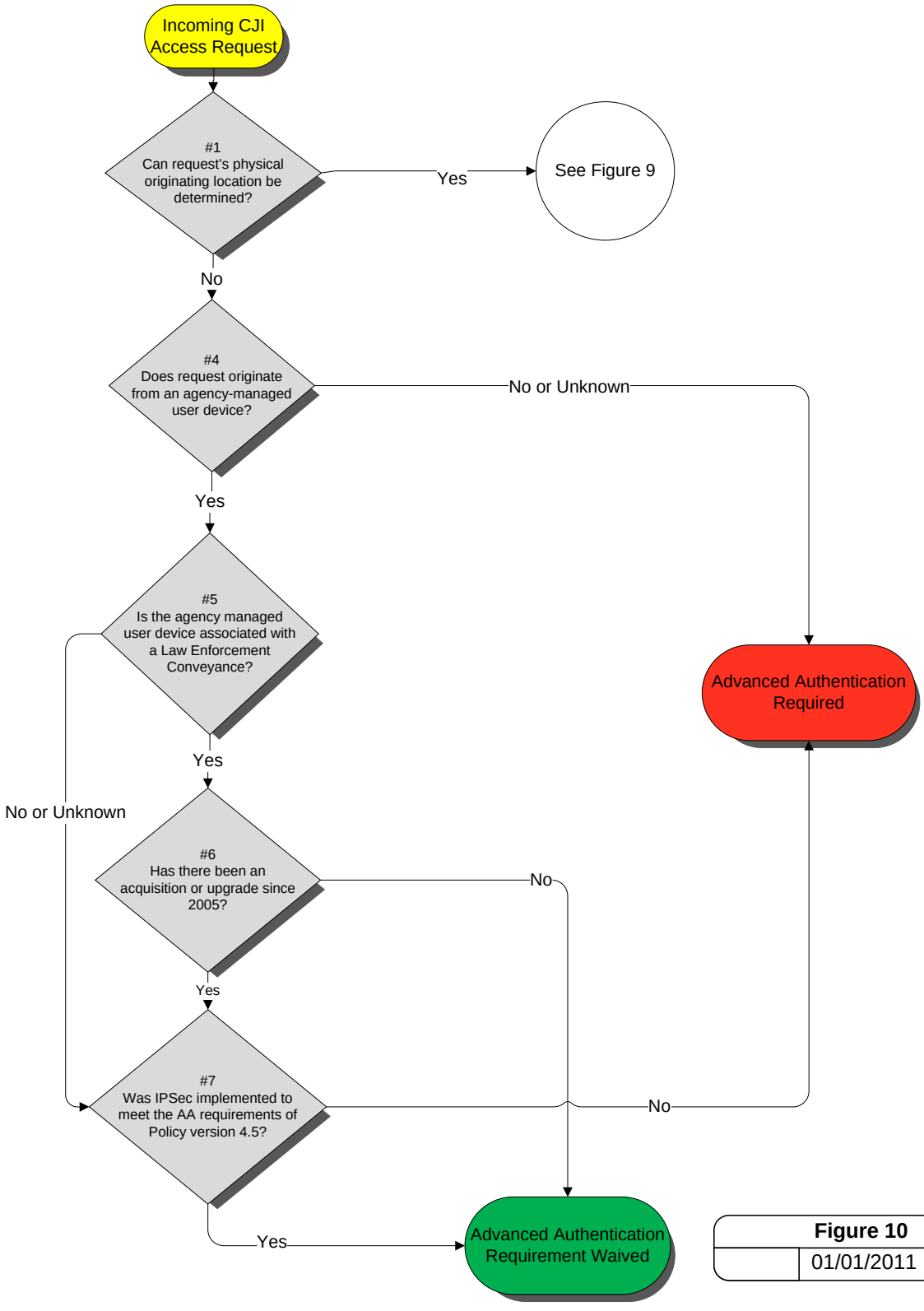


Figure 10
01/01/2011

5.7 Policy Area 7: Configuration Management

5.7.1 Access Restrictions for Changes

Planned or unplanned changes to the hardware, software, and/or firmware components of the information system can have significant effects on the overall security of the system. The goal is to allow only qualified and authorized individuals access to information system components for purposes of initiating changes, including upgrades, and modifications. Section 5.5, Access Control, describes agency requirements for control of privileges and restrictions.

5.7.1.1 Least Functionality

The agency shall configure the application, service, or information system to provide only essential capabilities and shall specifically prohibit and/or restrict the use of specified functions, ports, protocols, and/or services.

5.7.1.2 Network Diagram

The agency shall ensure that a complete topological drawing depicting the interconnectivity of the agency network, to criminal justice information, systems and services is maintained in a current status. See Appendix C for sample network diagrams.

The network topological drawing shall include the following:

1. All communications paths, circuits, and other components used for the interconnection, beginning with the agency-owned system(s) and traversing through all interconnected systems to the agency end-point.
2. The logical location of all components (e.g., firewalls, routers, switches, hubs, servers, encryption devices, and computer workstations). Individual workstations (clients) do not have to be shown; the number of clients is sufficient.
3. "For Official Use Only" (FOUO) markings.
4. The agency name and date (day, month, and year) drawing was created or updated.

5.7.2 Security of Configuration Documentation

The system configuration documentation often contains sensitive details (e.g. descriptions of applications, processes, procedures, data structures, authorization processes, data flow, etc.) Agencies shall protect the system documentation from unauthorized access consistent with the provisions described in section 5.5 Access Control.

5.7.3 References/Citations/Directives

Appendix I contains all of the references used in this policy and may contain additional sources that apply to this section.

Figure 11 – A Local Police Department's Configuration Management Controls

A local police department decided to update their CAD system, and in doing so tracked all changes made to their infrastructure in a configuration management journal, updated their network topology documents to include all new components in their architecture, then marked all documentation as FOUO and stored them securely.

5.8 Policy Area 8: Media Protection

Media protection policy and procedures shall be documented and implemented to ensure that access to electronic and physical media in all forms is restricted to authorized individuals. Procedures shall be defined for securely handling, transporting and storing media.

5.8.1 Media Storage and Access

The agency shall securely store electronic and physical media within physically secure locations or controlled areas. The agency shall restrict access to electronic and physical media to authorized individuals. If physical and personnel restrictions are not feasible then the data shall be encrypted per section 5.10.1.2.

5.8.2 Media Transport

The agency shall protect and control electronic and physical media during transport outside of controlled areas and restrict the activities associated with transport of such media to authorized personnel.

5.8.2.1 Electronic Media in Transit

"Electronic media" means electronic storage media including memory devices in laptops and computers (hard drives) and any removable, transportable digital memory media, such as magnetic tape or disk, optical disk, flash drives, external hard drives, or digital memory card.

Controls shall be in place to protect electronic media containing CJI while in transport (physically moved from one location to another) to help prevent compromise of the data. Encryption, as defined in section 5.10.1.2 of this policy, is the optimal control during transport; however, if encryption of the data isn't possible then each agency shall institute other controls to ensure the security of the data.

5.8.2.2 Physical Media in Transit

The controls and security measures in this document also apply to CJI in physical (printed documents, printed imagery, etc.) form. Physical media shall be protected at the same level as the information would be protected in electronic form.

5.8.3 Electronic Media Sanitization and Disposal

The agency shall sanitize, that is, overwrite at least three times or degauss electronic media prior to disposal or release for reuse by unauthorized individuals. Inoperable electronic media shall be destroyed (cut up, shredded, etc.). The agency shall maintain written documentation of the steps taken to sanitize or destroy electronic media. Agencies shall ensure the sanitization or destruction is witnessed or carried out by authorized personnel.

5.8.4 Disposal of Physical Media

Physical media shall be securely disposed of when no longer required, using formal procedures. Formal procedures for the secure disposal or destruction of physical media shall minimize the risk of sensitive information compromise by unauthorized individuals. Physical media shall be

destroyed by shredding or incineration. Agencies shall ensure the disposal or destruction is witnessed or carried out by authorized personnel.

5.8.5 References/Citations/Directives

Appendix I contains all of the references used in this policy and may contain additional sources that apply to this section.

Figure 12 – A Local Police Department's Media Management Policies

A local police department implemented a replacement CAD system that integrated to their state's CSA and was authorized to process CJI. The police department contracted with an off-site media manager to store backups of their data in the contractor's vaults, but the contractor was not authorized to process or store CJI. To ensure the confidentially of the police department's data while outside its perimeter, they encrypted all data going to the contractor with Advanced Encryption Standard (AES)-256. The police department rotated and reused media through the contractor's vaults periodically, and when it required destruction, the police department incinerated the media to irreversibly destroy any data on it.

5.9 Policy Area 9: Physical Protection

Physical protection policy and procedures shall be documented and implemented to ensure CJI and information system hardware, software, and media are physically protected through access control measures.

5.9.1 Physically Secure Location

A physically secure location is a facility or an area, a room, or a group of rooms within a facility with both the physical and personnel security controls sufficient to protect CJI and associated information systems. The physically secure location is subject to criminal justice agency management control; SIB control; FBI CJIS Security addendum; or a combination thereof.

Sections 5.9.1.1 – 5.9.1.9 describe the physical controls required in order to be considered a physically secure location, while section 5.12 describes the minimum personnel security controls required for unescorted access to a physically secure location. Section 5.6.2.2.1 describes the requirements for technical security controls required to access CJI within the perimeter of a physically secure location without AA.

For interim compliance, and for the sole purpose of meeting the advanced authentication policy, a police vehicle shall be considered a physically secure location until September 30th 2013. For the purposes of this policy, a police vehicle is defined as an enclosed criminal justice conveyance with the capability to comply, during operational periods, with section 5.9.1.3.

5.9.1.1 Security Perimeter

The perimeter of physically secure location shall be prominently posted and separated from non-secure locations by physical controls. Security perimeters shall be defined, controlled and secured in a manner acceptable to the CSA or SIB.

5.9.1.2 Physical Access Authorizations

The agency shall develop and keep current a list of personnel with authorized access to the physically secure location (except for those areas within the permanent facility officially designated as publicly accessible) or shall issue credentials to authorized personnel.

5.9.1.3 Physical Access Control

The agency shall control all physical access points (except for those areas within the facility officially designated as publicly accessible) and shall verify individual access authorizations before granting access.

5.9.1.4 Access Control for Transmission Medium

The agency shall control physical access to information system distribution and transmission lines within the physically secure location.

5.9.1.5 Access Control for Display Medium

The agency shall control physical access to information system devices that display CJI and shall position information system devices in such a way as to prevent unauthorized individuals from accessing and viewing CJI.

5.9.1.6 Monitoring Physical Access

The agency shall monitor physical access to the information system to detect and respond to physical security incidents.

5.9.1.7 Visitor Control

The agency shall control physical access by authenticating visitors before authorizing escorted access to the physically secure location (except for those areas designated as publicly accessible). The agency shall escort visitors at all times and monitor visitor activity.

5.9.1.8 Access Records

The agency shall maintain visitor access records to the physically secure location (except for those areas officially designated as publicly accessible) that includes:

1. Name and agency of the visitor.
2. Form of identification.
3. Date of access.
4. Time of entry and departure.
5. Purpose of visit.
6. Name and agency of person visited.

The visitor access records shall be maintained for a minimum of one year. Designated officials within the agency shall review the visitor access records frequently for accuracy and completeness.

5.9.1.9 Delivery and Removal

The agency shall authorize and control information system-related items entering and exiting the physically secure location.

5.9.2 Controlled Area

If an agency cannot meet all of the controls required for establishing a physically secure location, but has an operational need to access or store CJI, the agency shall designate an area, a room, or a storage container, as a controlled area for the purpose of day-to-day CJI access or storage. The agency shall, at a minimum:

1. Limit access to the controlled area during CJI processing times to only those personnel authorized by the agency to access or view CJI.
2. Lock the area, room, or storage container when unattended.
3. Position information system devices and documents containing CJI in such a way as to prevent unauthorized individuals from access and view.
4. Follow the encryption requirements found in section 5.10.1.2 for electronic storage (i.e. data “at rest”) of CJI.

5.9.3 References/Citations/Directives

Appendix I contains all of the references used in this policy and may contain additional sources that apply to this section.

Figure 13 – A Local Police Department's Physical Protection Measures

A local police department implemented a replacement CAD system that was authorized to process CJI over an encrypted VPN tunnel to the state's CSA. The police department established a physically separated wing within their precinct separated by locked doors, walls, and a monitored security system within which CJI was processed by dispatchers, officers, and detectives. Only those persons with the appropriate authorizations were permitted within this wing unless accompanied by such a person. Within this secure wing the police department further segregated the back-office information systems' infrastructure within a separately controlled area restricted only to those authorized administrative personnel with a need to enter.

5.10 Policy Area 10: System and Communications Protection and Information Integrity

Examples of systems and communications safeguards range from boundary and transmission protection to securing an agency's virtualized environment. In addition, applications, services, or information systems must have the capability to ensure system integrity through the detection and protection against unauthorized changes to software and information. This section details the policy for protecting systems and communications infrastructures.

5.10.1 Information Flow Enforcement

The network infrastructure shall control the flow of information between interconnected systems. Information flow control regulates where information is allowed to travel within an information system and between information systems (as opposed to who is allowed to access the information) and without explicit regard to subsequent accesses to that information. In other words, controlling how data moves from one place to the next in a secure manner. Examples of controls that are better expressed as flow control than access control (see section 5.5) are:

1. Prevent CJI from being transmitted unencrypted across the public network.
2. Block outside traffic that claims to be from within the agency.
3. Do not pass any web requests to the public network that are not from the internal web proxy.

Specific examples of flow control enforcement can be found in boundary protection devices (e.g. proxies, gateways, guards, encrypted tunnels, firewalls, and routers) that employ rule sets or establish configuration settings that restrict information system services or provide a packet filtering capability.

5.10.1.1 Boundary Protection

The agency shall:

1. Control access to networks processing CJI.
2. Monitor and control communications at the external boundary of the information system and at key internal boundaries within the system.
3. Ensure any connections to the Internet, other external networks, or information systems occur through controlled interfaces (e.g. proxies, gateways, routers, firewalls, encrypted tunnels). See Section 5.10.4.4 for guidance on personal firewalls.
4. Employ tools and techniques to monitor network events, detect attacks, and provide identification of unauthorized use.
5. Ensure the operational failure of the boundary protection mechanisms do not result in any unauthorized release of information outside of the information system boundary (i.e. the device shall "fail closed" vs. "fail open").
6. Allocate publicly accessible information system components (e.g. public Web servers) to separate sub networks with separate, network interfaces. Publicly accessible information

systems residing on a virtual host shall follow the guidance in section 5.10.3.2 to achieve separation.

5.10.1.2 Encryption

1. Encryption shall be a minimum of 128 bit.
2. When CJI is transmitted outside the boundary of the physically secure location, the data shall be immediately protected via cryptographic mechanisms (encryption).

   EXCEPTIONS: See sections 5.5.7.3.2 and 5.10.2.
3. When CJI is at rest (i.e. stored electronically) outside the boundary of the physically secure location, the data shall be protected via cryptographic mechanisms (encryption).
4. When encryption is employed, the cryptographic module used shall be certified to meet FIPS 140-2 standards.

   Note 1: Subsequent versions of approved cryptographic modules that are under current review for FIPS 140-2 compliancy can be used in the interim until certification is complete.

   Note 2: While FIPS 197 (Advanced Encryption Standard) certification is desirable, a FIPS 197 certification alone is insufficient as the certification is for the algorithm only vs. the FIPS 140-2 standard which certifies the packaging of an implementation.
5. For agencies using public key infrastructure technology, the agency shall develop and implement a certificate policy and certification practice statement for the issuance of public key certificates used in the information system. Registration to receive a public key certificate shall:
   a) Include authorization by a supervisor or a responsible official.
   b) Be accomplished by a secure process that verifies the identity of the certificate holder.
   c) Ensure the certificate is issued to the intended party.

5.10.1.3 Intrusion Detection Tools and Techniques

The agency shall implement network-based and/or host-based intrusion detection tools.

The CSA/SIB shall, in addition:

1. Monitor inbound and outbound communications for unusual or unauthorized activities.
2. Send individual intrusion detection logs to a central logging facility where correlation and analysis will be accomplished as a system wide intrusion detection effort.
3. Employ automated tools to support near-real-time analysis of events in support of detecting system-level attacks.

5.10.1.4 Voice over Internet Protocol

Voice over Internet Protocol (VoIP) has been embraced by organizations globally as an addition to, or replacement for, public switched telephone network (PSTN) and private branch exchange (PBX) telephone systems. The immediate benefits are lower costs than traditional telephone

services and VoIP can be installed in-line with an organization's existing Internet Protocol (IP) services. Among VoIP's risks that have to be considered carefully are: myriad security concerns, cost issues associated with new networking hardware requirements, and overarching quality of service (QoS) factors.

In addition to the security controls described in this document, the following additional controls shall be implemented when an agency deploys VoIP within a network that contains unencrypted CJI:

1. Establish usage restrictions and implementation guidance for VoIP technologies.
2. Change the default administrative password on the IP phones and VoIP switches.
3. Utilize Virtual Local Area Network (VLAN) technology to segment VoIP traffic from data traffic.

Appendix G.2 outlines threats, vulnerabilities, mitigations, and NIST best practices for VoIP.

5.10.2 Facsimile Transmission of CJI

CJI transmitted via facsimile is exempt from encryption requirements.

5.10.3 Partitioning and Virtualization

As resources grow scarce, agencies are increasing the centralization of applications, services, and system administration. Advanced software now provides the ability to create virtual machines that allows agencies to reduce the amount of hardware needed. Although the concepts of partitioning and virtualization have existed for a while, the need for securing the partitions and virtualized machines has evolved due to the increasing amount of distributed processing and federated information sources now available across the Internet.

5.10.3.1 Partitioning

The application, service, or information system shall separate user functionality (including user interface services) from information system management functionality.

The application, service, or information system shall physically or logically separate user interface services (e.g. public web pages) from information storage and management services (e.g. database management). Separation may be accomplished through the use of one or more of the following:

1. Different computers.
2. Different central processing units.
3. Different instances of the operating system.
4. Different network addresses.
5. Other methods approved by the FBI CJIS ISO.

5.10.3.2 Virtualization

Virtualization refers to a methodology of dividing the resources of a computer (hardware and software) into multiple execution environments. Virtualized environments are authorized for

criminal justice and noncriminal justice activities. In addition to the security controls described in this policy, the following additional controls shall be implemented in a virtual environment:

1. Isolate the host from the virtual machine. In other words, virtual machine users cannot access host files, firmware, etc.
2. Maintain audit logs for all virtual machines and hosts and store the logs outside the hosts' virtual environment.
3. Virtual Machines that are Internet facing (web servers, portal servers, etc.) shall be physically separate from Virtual Machines that process CJI internally.
4. Device drivers that are "critical" shall be contained within a separate guest.

The following are additional technical security control best practices and should be implemented wherever feasible:

1. Encrypt network traffic between the virtual machine and host.
2. Implement IDS and IPS monitoring within the virtual machine environment.
3. Virtually firewall each virtual machine from each other (or physically firewall each virtual machine from each other with an application layer firewall) and ensure that only allowed protocols will transact.
4. Segregate the administrative duties for the host.

Appendix G provides some reference and additional background information on virtualization.

5.10.4 System and Information Integrity Policy and Procedures

5.10.4.1 Patch Management

The agency shall identify applications, services, and information systems containing software or components affected by recently announced software flaws and potential vulnerabilities resulting from those flaws.

The agency (or the software developer/vendor in the case of software developed and maintained by a vendor/contractor) shall develop and implement a local policy that ensures prompt installation of newly released security relevant patches, service packs and hot fixes. Local policies should include such items as:

1. Testing of appropriate patches before installation.
2. Rollback capabilities when installing patches, updates, etc.
3. Automatic updates without individual user intervention.
4. Centralized patch management.

Patch requirements discovered during security assessments, continuous monitoring or incident response activities shall also be addressed expeditiously.

5.10.4.2 Malicious Code Protection

The agency shall implement malicious code protection that includes automatic updates for all systems with Internet access. Agencies with systems not connected to the Internet shall

implement local procedures to ensure malicious code protection is kept current (i.e. most recent update available).

The agency shall employ virus protection mechanisms to detect and eradicate malicious code (e.g., viruses, worms, Trojan horses) at critical points throughout the network and on all workstations, servers and mobile computing devices on the network. The agency shall ensure malicious code protection is enabled on all of the aforementioned critical points and information systems and resident scanning is employed.

5.10.4.3 Spam and Spyware Protection

The agency shall implement spam and spyware protection.

The agency shall:

1. Employ spam protection mechanisms at critical information system entry points (e.g. firewalls, electronic mail servers, remote-access servers).
2. Employ spyware protection at workstations, servers and/or mobile computing devices on the network.
3. Use the spam and spyware protection mechanisms to detect and take appropriate action on unsolicited messages and spyware/adware, respectively, transported by electronic mail, electronic mail attachments, Internet accesses, removable media (e.g. diskettes or compact disks) or other removable media as defined in this policy document.

5.10.4.4 Personal Firewall

A personal firewall shall be employed on all devices that are mobile by design (i.e. laptops, handhelds, personal digital assistants, etc.). For the purpose of this policy, a personal firewall is an application that controls network traffic to and from a user device, permitting or denying communications based on policy. At a minimum, the personal firewall shall perform the following activities:

1. Manage program access to the Internet.
2. Block unsolicited requests to connect to the user device.
3. Filter incoming traffic by IP address or protocol.
4. Filter incoming traffic by destination ports.
5. Maintain an IP traffic log.

5.10.4.5 Security Alerts and Advisories

The agency shall:

1. Receive information system security alerts/advisories on a regular basis.
2. Issue alerts/advisories to appropriate personnel.
3. Document the types of actions to be taken in response to security alerts/advisories.
4. Take appropriate actions in response.

5. Employ automated mechanisms to make security alert and advisory information available throughout the agency as appropriate.

5.10.4.6 Information Input Restrictions

The agency shall restrict the information input to any connection to FBI CJIS services to authorized personnel only.

Restrictions on personnel authorized to input information to the information system may extend beyond the typical access controls employed by the system and include limitations based on specific operational/project responsibilities.

5.10.5 References/Citations/Directives

Appendix I contains all of the references used in this policy and may contain additional sources that apply to this section.

Figure 14 – A Local Police Department's Information Systems & Communications Protections

A local police department implemented a replacement CAD system within a physically secure location that was authorized to process CJI using a FIPS 140-2 encrypted VPN tunnel over the Internet to the state's CSA. In addition to the policies, physical and personnel controls already in place, the police department employed firewalls both at their border and at key points within their network, intrusion detection systems, a patch-management strategy that included automatic patch updates where possible, virus scanners, spam and spyware detection mechanisms that update signatures automatically, and subscribed to various security alert mailing lists and addressed vulnerabilities raised through the alerts as needed.

5.11 Policy Area 11: Formal Audits

Formal audits are conducted to ensure compliance with applicable statutes, regulations and policies.

5.11.1 Audits by the FBI CJIS Division

5.11.1.1 Triennial Compliance Audits by the FBI CJIS Division

The FBI CJIS Division is authorized to conduct audits, once every three (3) years as a minimum, to assess agency compliance with applicable statutes, regulations and policies. The CJIS Audit Unit (CAU) shall conduct a triennial audit of each CSA in order to verify compliance with applicable statutes, regulations and policies. This audit shall include a sample of CJAs and, in coordination with the SIB, the NCJAs. Audits may be conducted on a more frequent basis if the audit reveals that an agency has not complied with applicable statutes, regulations and policies. The FBI CJIS Division shall also have the authority to conduct unannounced security inspections and scheduled audits of Contractor facilities.

5.11.1.2 Triennial Security Audits by the FBI CJIS Division

The FBI CJIS Division is authorized to conduct security audits of the CSA and SIB networks and systems, once every three (3) years as a minimum, to assess agency compliance with the CJIS Security Policy. This audit shall include a sample of CJAs and NCJAs. Audits may be conducted on a more frequent basis if the audit reveals that an agency has not complied with the CJIS Security Policy.

5.11.2 Audits by the CSA

Each CSA shall:

1. At a minimum, triennially audit all CJAs and NCJAs which have direct access to the state system in order to ensure compliance with applicable statutes, regulations and policies.
2. In coordination with the SIB, establish a process to periodically audit all NCJAs, with access to CJI, in order to ensure compliance with applicable statutes, regulations and policies.
3. Have the authority to conduct unannounced security inspections and scheduled audits of Contractor facilities.

5.11.3 Special Security Inquiries and Audits

All agencies having access to CJI shall permit an inspection team to conduct an appropriate inquiry and audit of any alleged security violations. The inspection team shall be appointed by the APB and shall include at least one representative of the CJIS Division. All results of the inquiry and audit shall be reported to the APB with appropriate recommendations.

5.11.4 References/Citations/Directives

Appendix I contains all of the references used in this policy and may contain additional sources that apply to this section.

Figure 15 – The Audit of a Local Police Department

A local police department implemented a replacement CAD system that integrated to their state's CSA and was authorized to process CJI. Shortly after the implementation, their state's CSA conducted an audit of their policies, procedures, and systems that process CJI. The police department supplied all architectural and policy documentation, including detailed network diagrams, to the auditors in order to assist them in the evaluation. The auditors discovered a deficiency in the police department's systems and marked them "out" in this aspect of the FBI CJIS Security Policy. The police department quickly addressed the deficiency and took corrective action, notifying the auditors of their actions.

5.12 Policy Area 12: Personnel Security

Having proper security measures against the insider threat is a critical component for the CJIS Security Policy. This section's security terms and requirements apply to all personnel who have access to unencrypted CJI including those individuals with only physical or logical access to devices that store, process or transmit unencrypted CJI.

5.12.1 Personnel Security Policy and Procedures

5.12.1.1 Minimum Screening Requirements for Individuals Requiring Access to CJI:

1. To verify identification, a state of residency and national fingerprint-based record checks shall be conducted within 30 days of assignment for all personnel who have direct access to CJI and those who have direct responsibility to configure and maintain computer systems and networks with direct access to CJI. However, if the person resides in a different state than that of the assigned agency, the agency shall conduct state (of the agency) and national fingerprint-based record checks and execute a NLETS CHRI IQ/FQ/AQ query using purpose code C, E, or J depending on the circumstances. When appropriate, the screening shall be consistent with:

   (i) 5 CFR 731.106; and/or

   (ii) Office of Personnel Management policy, regulations, and guidance; and/or

   (iii) agency policy, regulations, and guidance.

   (See Appendix J for applicable guidance regarding noncriminal justice agencies performing adjudication of civil fingerprint submissions.) Federal entities bypassing state repositories in compliance with federal law may not be required to conduct a state fingerprint-based record check.

2. All requests for access shall be made as specified by the CSO. The CSO, or their designee, is authorized to approve access to CJI. All CSO designees shall be from an authorized criminal justice agency.

3. If a felony conviction of any kind exists, the hiring authority in the Interface Agency shall deny access to CJI. However, the hiring authority may ask for a review by the CSO in extenuating circumstances where the severity of the offense and the time that has passed would support a possible variance.

4. If a record of any other kind exists, access to CJI shall not be granted until the CSO or his/her designee reviews the matter to determine if access is appropriate.

5. If the person appears to be a fugitive or has an arrest history without conviction, the CSO or his/her designee shall review the matter to determine if access to CJI is appropriate.

6. If the person is employed by a NCJA, the CSO or his/her designee, and, if applicable, the appropriate board maintaining management control, shall review the matter to determine if CJI access is appropriate. This same procedure applies if this person is found to be a fugitive or has an arrest history without conviction.

7. If the person already has access to CJI and is subsequently arrested and or convicted, continued access to CJI shall be determined by the CSO. This does not implicitly grant hiring/firing authority with the CSA, only the authority to grant access to CJI.
8. If the CSO or his/her designee determines that access to CJI by the person would not be in the public interest, access shall be denied and the person's appointing authority shall be notified in writing of the access denial.
9. Support personnel, contractors, and custodial workers with access to physically secure locations or controlled areas (during CJI processing) shall be subject to a state and national fingerprint-based record check unless these individuals are escorted by authorized personnel at all times.

It is recommended individual background re-investigations be conducted every five years unless Rap Back is implemented.

5.12.1.2 Personnel Screening for Contractors and Vendors

In addition to meeting the requirements in paragraph 5.12.1.1, contractors and vendors shall meet the following requirements:

1. Prior to granting access to CJI, the CGA on whose behalf the Contractor is retained shall verify identification via a state of residency and national fingerprint-based record check. However, if the person resides in a different state than that of the assigned agency, the agency shall conduct state (of the agency) and national fingerprint-based record checks and execute a NLETS CHRI IQ/FQ/AQ query using purpose code C, E, or J depending on the circumstances.
2. If a record of any kind is found, the CGA shall be formally notified and system access shall be delayed pending review of the criminal history record information. The CGA shall in turn notify the Contractor-appointed Security Officer.
3. When identification of the applicant with a criminal history has been established by fingerprint comparison, the CGA or the CJA (if the CGA does not have the authority to view CHRI) shall review the matter.
4. A Contractor employee found to have a criminal record consisting of felony conviction(s) shall be disqualified.
5. Applicants shall also be disqualified on the basis of confirmations that arrest warrants are outstanding for such applicants.
6. The CGA shall maintain a list of personnel who have been authorized access to CJI and shall, upon request, provide a current copy of the access list to the CSO.

Applicants with a record of misdemeanor offense(s) may be granted access if the CSO determines the nature or severity of the misdemeanor offense(s) do not warrant disqualification. The CGA may request the CSO to review a denial of access determination.

5.12.2 Personnel Termination

The agency, upon termination of individual employment, shall immediately terminate access to CJI.

5.12.3 Personnel Transfer

The agency shall review CJI access authorizations when personnel are reassigned or transferred to other positions within the agency and initiate appropriate actions such as closing and establishing accounts and changing system access authorizations.

5.12.4 Personnel Sanctions

The agency shall employ a formal sanctions process for personnel failing to comply with established information security policies and procedures.

5.12.5 References/Citations/Directives

Appendix I contains all of the references used in this policy and may contain additional sources that apply to this section.

Figure 16 – A Local Police Department's Personnel Security Controls

A local police department implemented a replacement CAD system that integrated to their state's CSA and was authorized to process CJI. In addition to the physical and technical controls already in place, the police department implemented a variety of personnel security controls to reduce the insider threat. The police department used background screening consistent with the FBI CJIS Security Policy to vet those with unescorted access to areas in which CJI is processed, including the IT administrators employed by a contractor and all janitorial staff. The police department established sanctions against any vetted person found to be in violation of stated policies. The police department re-evaluated each person's suitability for access to CJI every five years.

APPENDIX A TERMS AND DEFINITIONS

Access to Criminal Justice Information — The physical or logical (electronic) ability, right or privilege to view, modify or make use of Criminal Justice Information.

Administration of Criminal Justice — The detection, apprehension, detention, pretrial release, post-trial release, prosecution, adjudication, correctional supervision, or rehabilitation of accused persons or criminal offenders. It also includes criminal identification activities; the collection, storage, and dissemination of criminal history record information; and criminal justice employment. In addition, administration of criminal justice includes "crime prevention programs" to the extent access to criminal history record information is limited to law enforcement agencies for law enforcement programs (e.g. record checks of individuals who participate in Neighborhood Watch or "safe house" programs) and the result of such checks will not be disseminated outside the law enforcement agency.

Agency Coordinator (AC) — A staff member of the Contracting Government Agency who manages the agreement between the Contractor and agency.

Agency Liaison (AL) — Coordinator of activities between the criminal justice agency and the noncriminal justice agency when responsibility for a criminal justice system has been delegated by a criminal justice agency to a noncriminal justice agency, which has in turn entered into an agreement with a contractor. The agency liaison shall, inter alia, monitor compliance with system security requirements. In instances in which the noncriminal justice agency's authority is directly from the CJIS systems agency, there is no requirement for the appointment of an agency liaison.

Authorized User/Personnel — An individual, or group of individuals, who have been appropriately vetted through a national fingerprint-based record check and have been granted access to CJI data.

Authorized Recipient — (1) A criminal justice agency or federal agency authorized to receive CHRI pursuant to federal statute or executive order; (2) A nongovernmental entity authorized by federal statute or executive order to receive CHRI for noncriminal justice purposes; or (3) A government agency authorized by federal statute or executive order, or state statute which has been approved by the United States Attorney General to receive CHRI for noncriminal justice purposes.

Availability — The degree to which information, a system, subsystem, or equipment is operable and in a useable state; frequently represented as a proportion of time the element is in a functioning condition.

Biographic Data — Information collected about individuals associated with a unique case, and not necessarily connected to identity data. Biographic Data does not provide a history of an individual, only information related to a unique case.

Biometric Data — When applied to CJI, it is used to identify individuals, and includes the following types: finger prints, palm prints, DNA, iris, and facial recognition.

Case / Incident History — All relevant information gathered about an individual, organization, incident, or combination thereof, arranged so as to serve as an organized record to provide

analytic value for a criminal justice organization. In regards to CJI, it is the information about the history of criminal incidents.

Channeler — An FBI approved contractor, who has entered into an agreement with an Authorized Recipient(s), to receive noncriminal justice applicant fingerprint submissions and collect the associated fees. The Channeler ensures fingerprint submissions are properly and adequately completed, electronically forwards fingerprint submissions to the FBI's CJIS Division for national noncriminal justice criminal history record check, and receives electronic record check results for dissemination to Authorized Recipients. A Channeler is essentially an "expediter" rather than a user of criminal history record check results.

CJIS Advisory Policy Board (APB) — The governing organization within the FBI CJIS Advisory Process composed of representatives from criminal justice and national security agencies within the United States. The APB reviews policy, technical, and operational issues relative to CJIS Division programs and makes subsequent recommendations to the Director of the FBI.

CJIS Audit Unit (CAU) — The organization within the FBI CJIS Division responsible to perform audits of CSAs to verify compliance with the CJIS Security Policy**.**

CJIS Security Policy — The FBI CJIS Security Policy document as published by the FBI CJIS ISO; the document containing this glossary.

CJIS Systems Agency (CSA) — A duly authorized state, federal, international, tribal, or territorial criminal justice agency on the CJIS network providing statewide (or equivalent) service to its criminal justice users with respect to the CJIS data from various systems managed by the FBI CJIS Division. There shall be only one CSA per state or territory. In federal agencies, the CSA may be the interface or switch to other federal agencies connecting to the FBI CJIS systems.

CJIS Systems Agency Information Security Officer (CSA ISO) — The appointed FBI CJIS Division personnel responsible to coordinate information security efforts at all CJIS interface agencies.

CJIS Systems Officer (CSO) — An individual located within the CJIS Systems Agency responsible for the administration of the CJIS network on behalf for the CJIS Systems Agency.

Compact Council — The entity created by the National Crime Prevention and Privacy Compact of 1998 that has the authority to promulgate rules and procedures governing the use of the III system for noncriminal justice purposes.

Compact Officers — The leadership of the Compact Council, oversees the infrastructure established by the National Crime Prevention and Privacy Compact Act of 1998, which is used by ratifying states to exchange criminal records for noncriminal justice purposes. Their primary responsibilities are to promulgate rules and procedures for the effective and appropriate use of the III system.

Computer Security Incident Response Capability (CSIRC) — A collection of personnel, systems, and processes that are used to efficiently and quickly manage a centralized response to any sort of computer security incident which may occur.

Confidentiality — The concept of ensuring that information is observable only to those who have been granted authorization to do so.

Contractor — A private business, agency or individual which has entered into an agreement for the administration of criminal justice or noncriminal justice functions with a Criminal Justice Agency or a Noncriminal Justice Agency. Also, a private business approved by the FBI CJIS Division to contract with Noncriminal Justice Agencies to perform noncriminal justice functions associated with civil fingerprint submission for hiring purposes.

Contracting Government Agency (CGA) — The government agency, whether a Criminal Justice Agency or a Noncriminal Justice Agency, which enters into an agreement with a private contractor.

Crime Reports Data — The data collected through the Uniform Crime Reporting program and reported upon annually by the FBI CJIS division used to analyze the crime statistics for the United States.

Criminal History Record Information (CHRI) — A subset of CJI. Any notations or other written or electronic evidence of an arrest, detention, complaint, indictment, information or other formal criminal charge relating to an identifiable person that includes identifying information regarding the individual as well as the disposition of any charges.

Criminal Justice Agency (CJA) — The courts, a governmental agency, or any subunit of a governmental agency which performs the administration of criminal justice pursuant to a statute or executive order and which allocates a substantial part of its annual budget to the administration of criminal justice. State and federal Inspectors General Offices are included.

Criminal Justice Agency User Agreement — A terms-of-service agreement that must be signed prior to accessing CJI. This agreement is required by each CJA and spells out user's responsibilities, the forms and methods of acceptable use, penalties for their violation, disclaimers, and so on.

Criminal Justice Conveyance — A criminal justice conveyance is any mobile vehicle used for the purposes of criminal justice activities with the capability to comply, during operational periods, with the requirements of section 5.9.1.3.

Criminal Justice Information (CJI) — Criminal Justice Information is the abstract term used to refer to all of the FBI CJIS provided data necessary for law enforcement agencies to perform their mission and enforce the laws, including but not limited to: biometric, identity history, person, organization, property, and case/incident history data. In addition, CJI refers to the FBI CJIS-provided data necessary for civil agencies to perform their mission; including, but not limited to data used to make hiring decisions.

Criminal Justice Information Services Division (FBI CJIS or CJIS) — The FBI division responsible for the collection, warehousing, and timely dissemination of relevant CJI to the FBI and to qualified law enforcement, criminal justice, civilian, academic, employment, and licensing agencies.

Data — See Information and CJI.

Degauss — Neutralize a magnetic field to erase information from a magnetic disk or other storage device. In the field of information technology, degauss has become synonymous with erasing information whether or not the medium is magnetic. In the event the device to be degaussed is not magnetic (e.g. solid state drive, USB storage device), steps other than magnetic degaussing may be required to render the information irretrievable from the device.

Department of Justice (DoJ) — The Department within the U.S. Government responsible to enforce the law and defend the interests of the United States according to the law, to ensure public safety against threats foreign and domestic, to provide federal leadership in preventing and controlling crime, to seek just punishment for those guilty of unlawful behavior, and to ensure fair and impartial administration of justice for all Americans.

Digital Signature – A digital signature consists of three algorithms: (1) A key generation algorithm that selects a private key uniformly at random from a set of possible private keys. The algorithm outputs the private key and a corresponding public key. (2) A signing algorithm that, given a message and a private key, produces a signature. (3) A signature verifying algorithm that, given a message, public key, and a signature, either accepts or rejects the message's claim to authenticity. Two main properties are required. First, a signature generated from a fixed message and fixed private key should verify the authenticity of that message by using the corresponding public key. Secondly, it should be computationally infeasible to generate a valid signature for a party who does not possess the private key.

Direct Access — (1) Having the authority to access systems managed by the FBI CJIS Division, whether by manual or automated methods, not requiring the assistance of, or intervention by, any other party or agency (28 CFR, Chapter 1, Part 20). (2) Having the authority to query or update national databases maintained by the FBI CJIS Division including national queries and updates automatically or manually generated by the CSA.

Dissemination — The transmission/distribution of CJI to Authorized Recipients within an agency.

Escort – Authorized personnel who accompany a visitor at all times while within a physically secure location to ensure the protection and integrity of the physically secure location and any Criminal Justice Information therein. The use of cameras or other electronic means used to monitor a physically secure location does not constitute an escort.

Federal Bureau of Investigation (FBI) — The agency within the DOJ responsible to protect and defend the United States against terrorist and foreign intelligence threats, to uphold and enforce the criminal laws of the United States, and to provide leadership and criminal justice services to federal, state, municipal, and international agencies and partners.

FBI CJIS Information Security Officer (FBI CJIS ISO) — The FBI personnel responsible for the maintenance and dissemination of the FBI CJIS Security Policy; the liaison between the FBI and the CSA's ISOs and other relevant security points-of-contact (POCs); the provider of technical guidance as to the intent and implementation of technical policy issues; the POC for computer incident notification which also disseminates security alerts to the CSOs and ISOs.

Federal Information Security Management Act (FISMA) — The Federal Information Security Management Act of 2002, a US Federal law that established information security standards for the protection of economic and national security interests of the United States. It requires each federal agency to develop, document, and implement an agency-wide program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source.

For Official Use Only (FOUO) — A caveat applied to unclassified sensitive information that may be exempt from mandatory release to the public under the Freedom of Information Act

(FOIA), 5 U.S.C 522. In general, information marked FOUO shall not be disclosed to anybody except Government (Federal, State, tribal, or local) employees or contractors with a need to know.

Guest Operating System — An operating system that has emulated hardware presented to it by a host operating system. Also referred to as the virtualized operating system.

Host Operating System — In the context of virtualization, the operating system that interfaces with the actual hardware and arbitrates between it and the guest operating systems. It is also referred to as a hypervisor.

Hypervisor — See Host Operating System.

Identity History Data — Textual data that corresponds with an individual's biometric data, providing a history of criminal and/or civil events for the identified individual.

Information — See data and CJI.

Information Exchange Agreement — An agreement that codifies the rules by which two parties engage in the sharing of information. These agreements typically include language which establishes some general duty-of-care over the other party's information, whether and how it can be further disseminated, penalties for violations, the laws governing the agreement (which establishes venue), procedures for the handling of shared information at the termination of the agreement, and so on. This document will ensure consistency with applicable federal laws, directives, policies, regulations, standards and guidance.

Information Security Officer (ISO) — Typically a member of an organization who has the responsibility to establish and maintain information security policy, assesses threats and vulnerabilities, performs risk and control assessments, oversees the governance of security operations, and establishes information security training and awareness programs. The ISO also usually interfaces with security operations to manage implementation details and with auditors to verify compliance to established policies.

Information System — A system of people, data, and processes, whether manual or automated, established for the purpose of managing information.

Integrated Automated Fingerprint Identification System (IAFIS) — The national fingerprint and criminal history system maintained by the FBI CJIS Division that provides the law enforcement community with automated fingerprint search capabilities, latent searching capability, electronic image storage, and electronic exchange of fingerprints and responses.

Integrity — The perceived consistency of expected outcomes, actions, values, and methods of an individual or organization. As it relates to data, it is the concept that data is preserved in a consistent and correct state for its intended use.

Interconnection Security Agreement (ISA) — An agreement much like an Information Exchange Agreement as mentioned above, but concentrating more on formalizing the technical and security requirements pertaining to some sort of interface between the parties' information systems.

Interface Agency — A legacy term used to describe agencies with direct connections to the CSA. This term is now used predominantly in a common way to describe any sub-agency of a CSA or SIB that leverages the CSA or SIB as a conduit to FBI CJIS information.

Internet Protocol (IP) — A protocol used for communicating data across a packet-switched internetwork using the Internet Protocol Suite, also referred to as TCP/IP. IP is the primary protocol in the Internet Layer of the Internet Protocol Suite and has the task of delivering distinguished protocol datagrams (packets) from the source host to the destination host solely based on their addresses.

Interstate Identification Index (III) — The CJIS service that manages automated submission and requests for CHRI that is warehoused subsequent to the submission of fingerprint information. Subsequent requests are directed to the originating State as needed.

Law Enforcement Online (LEO) — A secure, Internet-based communications portal provided by the FBI CJIS Division for use by law enforcement, first responders, criminal justice professionals, and anti-terrorism and intelligence agencies around the globe. Its primary purpose is to provide a platform on which various law enforcement agencies can collaborate on FOUO matters.

Logical Access – The technical means (e.g., read, create, modify, delete a file, execute a program, or use an external connection) for an individual or other computer system to utilize CJI or CJIS applications.

Local Agency Security Officer (LASO) — The primary Information Security contact between a local law enforcement agency and the CSA under which this agency interfaces with the FBI CJIS Division. The LASO actively represents their agency in all matters pertaining to Information Security, disseminates Information Security alerts and other material to their constituents, maintains Information Security documentation (including system configuration data), assists with Information Security audits of hardware and procedures, and keeps the CSA informed as to any Information Security needs and problems.

Management Control Agreement (MCA) — An agreement between parties that wish to share or pool resources that codifies precisely who has administrative control over, versus overall management and legal responsibility for, assets covered under the agreement. An MCA must ensure the CJA's authority remains with regard to all aspects of section 3.2.2. The MCA usually results in the CJA having ultimate authority over the CJI supporting infrastructure administered by the NCJA.

National Crime Information Center (NCIC) — An information system which stores CJI which can be queried by appropriate Federal, state, and local law enforcement and other criminal justice agencies.

National Instant Criminal Background Check System (NICS) — A system mandated by the Brady Handgun Violence Prevention Act of 1993 that is used by Federal Firearms Licensees (FFLs) to instantly determine via telephone or other electronic means whether the transfer of a firearm would be in violation of Section 922 (g) or (n) of Title 18, United States Code, or state law, by evaluating the prospective buyer's criminal history.

National Institute of Standards and Technology (NIST) — Founded in 1901, NIST is a non-regulatory federal agency within the U.S. Department of Commerce whose mission is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic and national security.

Noncriminal Justice Agency (NCJA) — A governmental agency, or any subunit thereof, that provides services primarily for purposes other than the administration of criminal justice.

Examples of services include, but not limited to, employment suitability, licensing determinations, immigration and naturalization matters, and national security clearances.

NCJA (Government) — A Federal, state, local, or tribal governmental agency or any subunit thereof whose charter does not include the responsibility to administer criminal justice, but may have a need to process CJI. An example would be the central IT organization within a state government that administers equipment on behalf of a state law-enforcement agency.

NCJA (Private) — A private agency or subunit thereof whose charter does not include the responsibility to administer criminal justice, but may have a need to process CJI. An example would include a local bank.

NCJA (Public) — A public agency or sub-unit thereof whose charter does not include the responsibility to administer criminal justice, but may have a need to process CJI. An example would include a county school board which uses CHRI to assist in employee hiring decisions.

Noncriminal Justice Purpose — The uses of criminal history records for purposes authorized by federal or state law other than purposes relating to the administration of criminal justice, including employment suitability, licensing determinations, immigration and naturalization matters, and national security clearances.

Office of Management and Budget (OMB) — The agency within the Executive Branch of the Federal government responsible to oversee the preparation of the federal budget, to assist in the supervision of other Executive Branch agencies, and to oversee and coordinate the Presidential Administration's procurement, financial management, information, and regulatory policies.

Outsourcing — The process of delegating in-house operations to a third-party. For instance, when the administration of criminal justice functions (network operations, dispatch functions, system administration operations, etc.) are performed for the criminal justice agency by a city or county information technology department or are contracted to be performed by a vendor.

Outsourcing Standard — National Crime Prevention and Privacy Compact Council's Outsourcing Standard. The Compact Council's uniform standards and processes for the interstate and Federal-State exchange of criminal history records for noncriminal justice purposes.

Physical Access – The physical ability, right or privilege to view, modify or make use of Criminal Justice Information (CJI) by means of physical presence within the proximity of computers and network devices (e.g. the ability to insert a boot disk or other device into the system, make a physical connection with electronic equipment, etc.).

Physically Secure Location — A facility or an area, a room, or a group of rooms, within a facility with both the physical and personnel security controls sufficient to protect CJI and associated information systems. For interim compliance, a police vehicle shall be considered a physically secure location until September 30th, 2013. For the purposes of this policy, a police vehicle is defined as an enclosed criminal justice conveyance with the capability to comply, during operational periods, with section 5.9.1.3.

Personal Firewall — An application which controls network traffic to and from a computer, permitting or denying communications based on a security policy.

Personally Identifiable Information (PII) — PII is information which can be used to distinguish or trace an individual's identity, such as name, social security number, or biometric

records, alone or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, or mother's maiden name.

Property Data — Information about vehicles and property associated with a crime.

Rap Back — An IAFIS service that allows authorized agencies to receive notification of subsequent criminal activity reported to the FBI committed by persons of interest.

Repository Manager — The designated manager of the agency having oversight responsibility for a CSA's fingerprint identification services. If both state fingerprint identification services and CJIS systems control are managed within the same state agency, the repository manager and CSO may be the same person.

Secondary Dissemination — The promulgation of CJI from a releasing agency to an authorized recipient agency when the recipient agency has not been previously identified in a formal information exchange agreement.

Security Addendum (SA) — A uniform addendum to an agreement between the government agency and a private contractor, approved by the Attorney General of the United States, which specifically authorizes access to criminal history record information, limits the use of the information to the purposes for which it is provided, ensures the security and confidentiality of the information consistent with existing regulations and the CJIS Security Policy, provides for sanctions, and contains such other provisions as the Attorney General may require.

Sensitive But Unclassified (SBU) — Designation of information in the United States federal government that, though unclassified, often requires strict controls over its distribution. SBU is a broad category of information that includes material covered by such designations as For Official Use Only (FOUO), Law Enforcement Sensitive (LES), Sensitive Homeland Security Information, Security Sensitive Information (SSI), Critical Infrastructure Information (CII), etc. Some categories of SBU information have authority in statute or regulation (e.g. SSI, CII) while others, including FOUO, do not. As of May 9, 2008, the more appropriate terminology to use is Controlled Unclassified Information (CUI).

Service — The organized system of apparatus, appliances, personnel, etc, that supply some tangible benefit to the consumers of this service. In the context of CJI, this usually refers to one of the applications that can be used to process CJI.

Shredder — A device used for shredding documents, often as a security measure to prevent unapproved persons from reading them. Strip-cut shredders, also known as straight-cut or spaghetti-cut, slice the paper into long, thin strips but are not considered secure. Cross-cut shredders provide more security by cutting paper vertically and horizontally into confetti-like pieces.

Social Engineering — The act of manipulating people into performing actions or divulging confidential information. While similar to a confidence trick or simple fraud, the term typically applies to trickery or deception for the purpose of information gathering, fraud, or computer system access; in most cases the attacker never comes face-to-face with the victim.

Software Patch — A piece of software designed to fix problems with, or update, a computer program or its supporting data. This includes fixing security vulnerabilities and other bugs and improving the usability or performance. Though meant to fix problems, poorly designed patches can sometimes introduce new problems. As such, patches should be installed in a test

environment prior to being installed in a live, operational system. Patches often can be found in multiple locations but should be retrieved only from sources agreed upon through organizational policy.

State and Federal Agency User Agreement — A written agreement that each CSA or SIB Chief shall execute with the FBI CJIS Division stating their willingness to demonstrate conformance with the FBI CJIS Security Policy prior to the establishment of connectivity between organizations. This agreement includes the standards and sanctions governing use of CJIS systems, as well as verbiage to allow the FBI to periodically audit the CSA as well as to allow the FBI to penetration test its own network from the CSA's interfaces to it.

State Compact Officer — The representative of a state that is party to the National Crime Prevention and Privacy Compact, and is the chief administrator of the state's criminal history record repository or a designee of the chief administrator who is a regular full-time employee of the repository.

State Identification Bureau (SIB) — The state agency with the responsibility for the state's fingerprint identification services.

State Identification Bureau (SIB) Chief — The SIB Chief is the designated manager of state's SIB. If both state fingerprint identification services and CJIS systems control are managed within the same state agency, the SIB Chief and CSO may be the same person.

State of Residency – A state of residency is the state in which an individual claims and can provide documented evidence as proof of being his/her permanent living domicile. Examples of acceptable documented evidence permitted to confirm an individual's state of residence are: driver's license, state or employer issued ID card, voter registration card, proof of an address (such as a utility bill with one's name and address as the payee), passport, professional or business license, and/or insurance (medical/dental) card.

System — Refer to connections to the FBI's criminal justice information repositories and the equipment used to establish said connections. In the context of CJI, this usually refers to applications and all interconnecting infrastructure required to use those applications that process CJI.

Terminal Agency Coordinator (TAC) — Serves as the point-of-contact at the local agency for matters relating to CJIS information access. A TAC administers CJIS systems programs within the local agency and oversees the agency's compliance with CJIS systems policies.

Virtualization — Refers to a methodology of dividing the resources of a computer (hardware and software) into multiple execution environments, by applying one or more concepts or technologies such as hardware and software partitioning, time-sharing, partial or complete machine simulation or emulation allowing multiple operating systems, or images, to run concurrently on the same hardware.

Voice over Internet Protocol (VoIP) — A set of software, hardware, and standards designed to make it possible to transmit voice over packet switched networks, either an internal Local Area Network, or across the Internet.

APPENDIX B ACRONYMS

Acronym	Term
AA	Advanced Authentication
AC	Agency Coordinator
ACL	Access Control List
AES	Advanced Encryption Standard
AP	Access Point
APB	Advisory Policy Board
BD-ADDR	Bluetooth-Enabled Wireless Devices and Addresses
CAD	Computer-Assisted Dispatch
CAU	CJIS Audit Unit
CFR	Code of Federal Regulations
CGA	Contracting Government Agency
CHRI	Criminal History Record Information
CJA	Criminal Justice Agency
CJI	Criminal Justice Information
CJIS	Criminal Justice Information Services
ConOps	Concept of Operations
CSA	CJIS Systems Agency
CSIRC	Computer Security Incident Response Capability
CSO	CJIS Systems Officer
DAA	Designated Approving Authority
DoJ	Department of Justice
DoJCERT	DoJ Computer Emergency Response Team

FBI	Federal Bureau of Investigation
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
FOIA	Freedom of Information Act
FOUO	For Official Use Only
HTTP	Hypertext Transfer Protocol
IAFIS	Integrated Automated Fingerprint Identification System
IDS	Intrusion Detection System
III	Interstate Identification Index
IP	Internet Protocol
IPS	Intrusion Prevention System
IPSEC	Internet Protocol Security
ISA	Interconnection Security Agreement
ISO	Information Security Officer
IT	Information Technology
LASO	Local Agency Security Officer
LEO	Law Enforcement Online
MAC	Media Access Control
MCA	Management Control Agreement
MITM	Man-in-the-Middle
MOU	Memorandum of Understanding
NCIC	National Crime Information Center
NCJA	Noncriminal Justice Agency
NICS	National Instant Criminal Background Check System
NIST	National Institute of Standards and Technology

OMB	Office of Management and Budget
ORI	Originating Agency Identifier
PBX	Private Branch Exchange
PDA	Personal Digital Assistant
PII	Personally Identifiable Information
PIN	Personal Identification Number
PKI	Public Key Infrastructure
POC	Point-of-Contact
PSTN	Public Switched Telephone Network
QA	Quality Assurance
QoS	Quality of Service
RF	Radio Frequency
SA	Security Addendum
SCO	State Compact Officer
SIB	State Identification Bureau
SIG	Special Interest Group
SP	Special Publication
SSID	Service Set Identifier
TAC	Terminal Agency Coordinator
TLS	Transport Layer Security
VLAN	Virtual Local Area Network
VoIP	Voice Over Internet Protocol
VPN	Virtual Private Network
WEP	Wired Equivalent Privacy
WLAN	Wireless Local Area Network

WPA	Wi-Fi Protected Access

APPENDIX C NETWORK TOPOLOGY DIAGRAMS

Network diagrams, i.e. topological drawings, are an essential part of solid network security. Through graphical illustration, a comprehensive network diagram provides the "big picture" – enabling network managers to quickly ascertain the interconnecting nodes of a network for a multitude of purposes, including troubleshooting and optimization. Network diagrams are integral to demonstrating the manner in which each agency ensures criminal justice data is afforded appropriate technical security protections and is protected during transit and at rest.

The following diagrams, labeled Appendix C.1-A through C.1-D, are examples for agencies to utilize during the development, maintenance, and update stages of their own network diagrams. By using these example drawings as a guideline, agencies can form the foundation for ensuring compliance with Section 5.7.1.2 of the CJIS Security Policy.

The purpose for including the following diagrams in this policy is to aid agencies in their understanding of diagram expectations and should not be construed as a mandated method for network topologies. It should also be noted that agencies are not required to use the identical icons depicted in the example diagrams and should not construe any depiction of a particular vendor product as an endorsement of that product by the FBI CJIS Division.

Appendix C.1-A is a conceptual overview of the various types of agencies that can be involved in handling of CJIS data, and illustrates several ways in which these interconnections might occur. This diagram is not intended to demonstrate the level of detail required for any given agency's documentation, but it provides the reader with some additional context through which to digest the following diagrams. Take particular note of the types of network interfaces in use between agencies, in some cases dedicated circuits with encryption mechanisms, and in other cases VPNs over the Internet. This diagram attempts to show the level of diversity possible within the law enforcement community. These diagrams in no way constitute a standard for network engineering, but rather, for the expected quality of documentation.

The next three topology diagrams, C.1-B through C.1-D, depict conceptual agencies. For C.1-B through C.1-D, the details identifying specific "moving parts" in the diagrams by manufacturer and model are omitted, but it is expected that any agencies producing such documentation will provide diagrams with full manufacturer and model detail for each element of the diagram. Note that the quantities of clients should be documented in order to assist the auditor in understanding the scale of assets and information being protected.

Appendix C.1-B depicts a conceptual state law enforcement agency's network topology and demonstrates a number of common technologies that are in use throughout the law enforcement community (some of which are compulsory per CJIS policy, and some of which are optional) including Mobile Broadband cards, VPNs, Firewalls, Intrusion Detection Devices, VLANs, and so forth. Note that although most state agencies will likely have highly-available configurations, the example diagram shown omits these complexities and only shows the "major moving parts" for clarity but please note the policy requires the logical location of all components be shown. The level of detail depicted should provide the reader with a pattern to model future documentation from, but should not be taken as network engineering guidance.

Appendix C.1-C depicts a conceptual county law enforcement agency. A number of common technologies are presented merely to reflect the diversity in the community, including proprietary

Packet-over-RF infrastructures and advanced authentication techniques, and to demonstrate the fact that agencies can act as proxies for other agencies.

Appendix C.1-D depicts a conceptual municipal law enforcement agency, presumably a small one that lacks any precinct-to-patrol data communications. This represents one of the smallest designs that could be assembled that, assuming all other details are properly considered, would meet the criteria for Section 5.7.1.2. This diagram helps to demonstrate the diversity in size that agencies handling criminal justice data exhibit.

Figure C-1-A Overview: Conceptual Connections Between Various Agencies

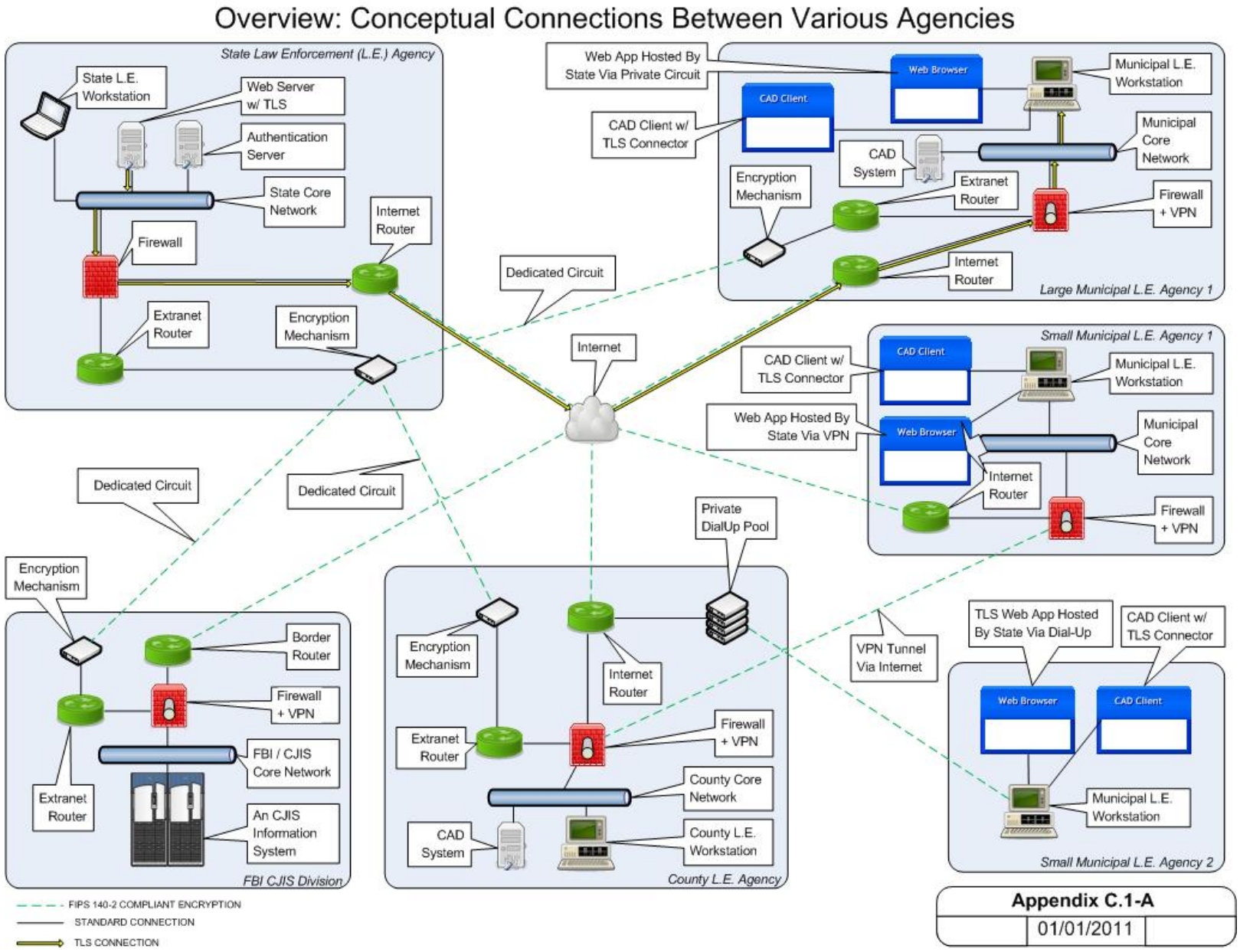
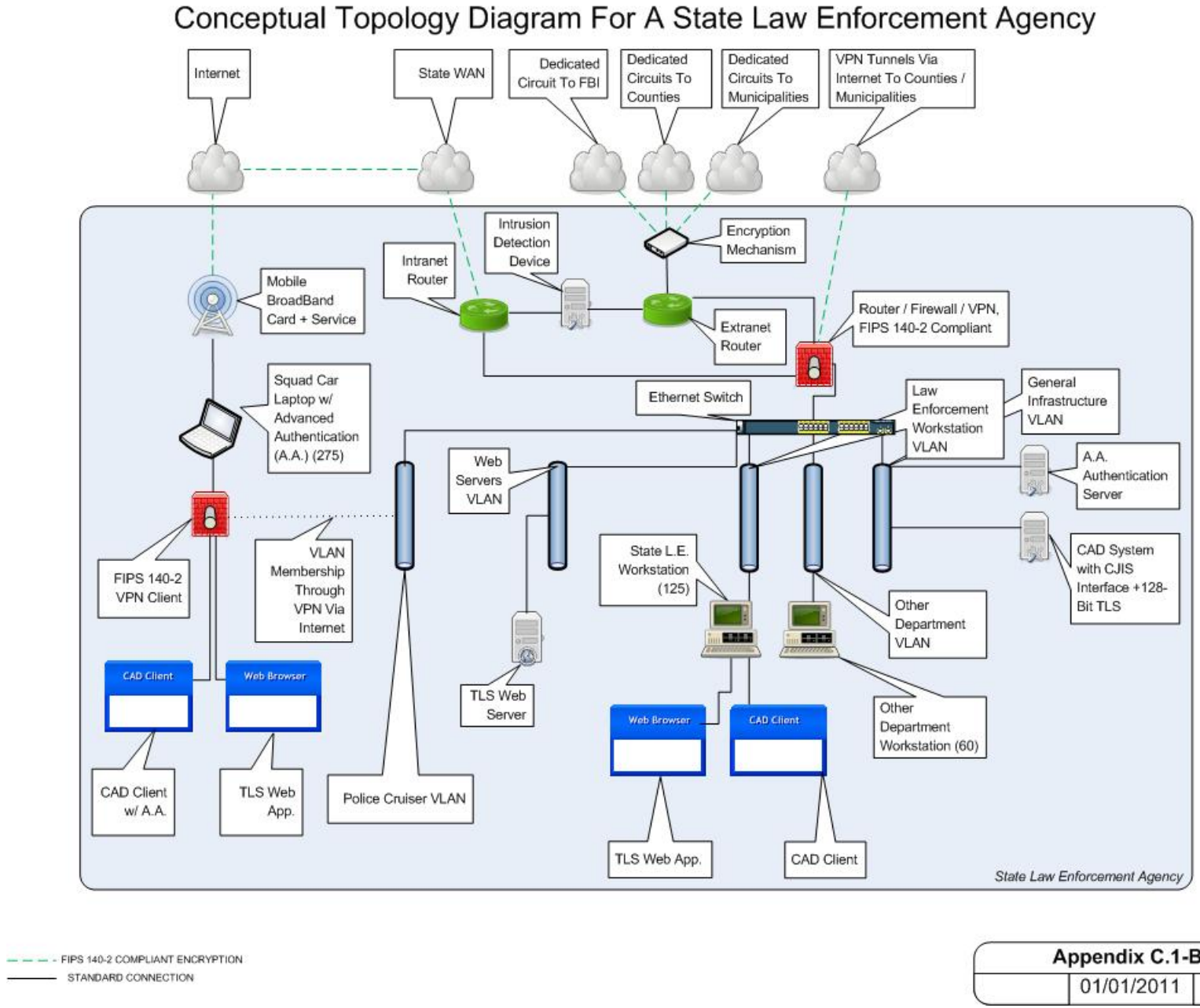
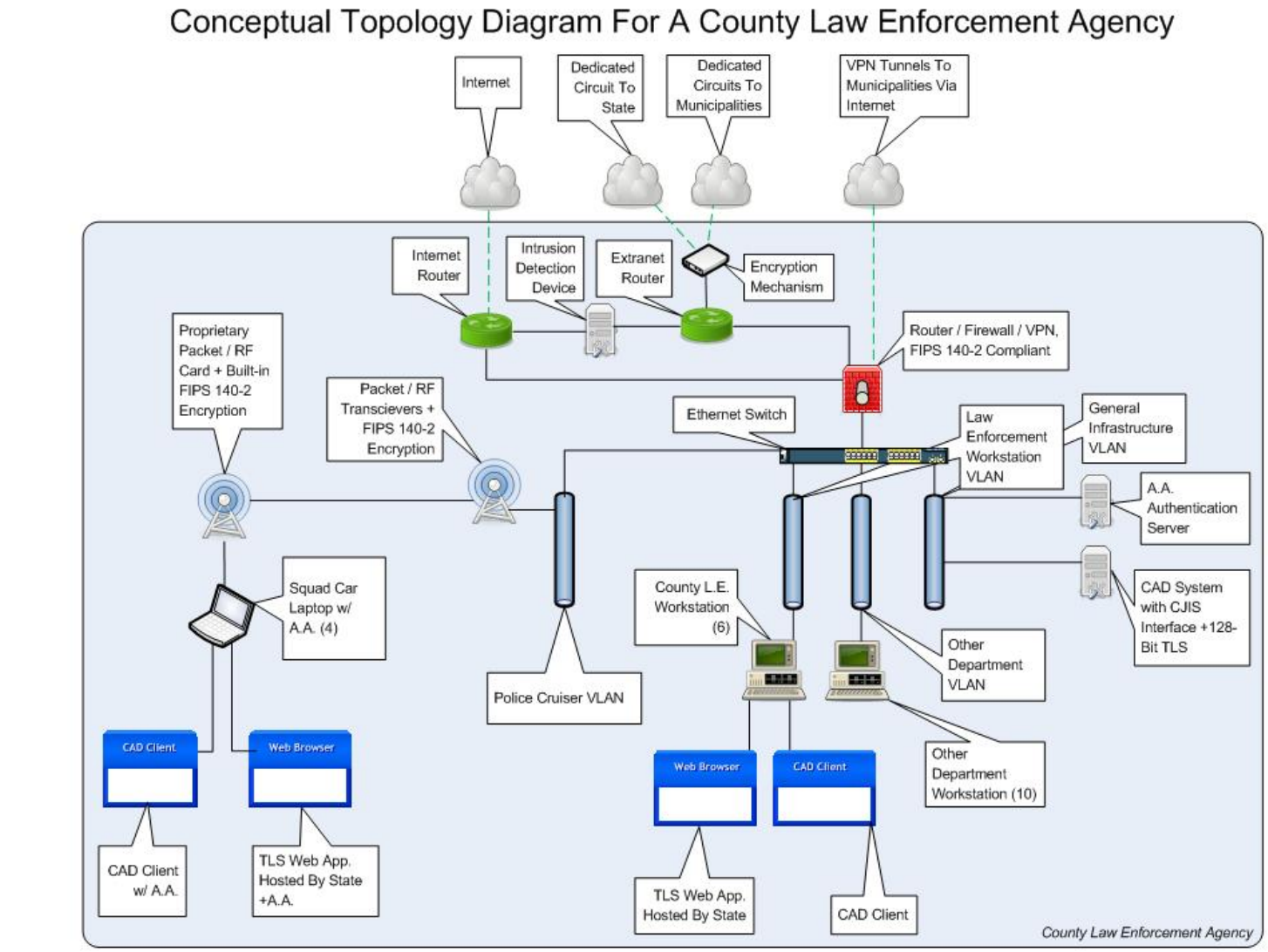


Figure C-1-B Conceptual Topology Diagram for a State Law Enforcement Agency



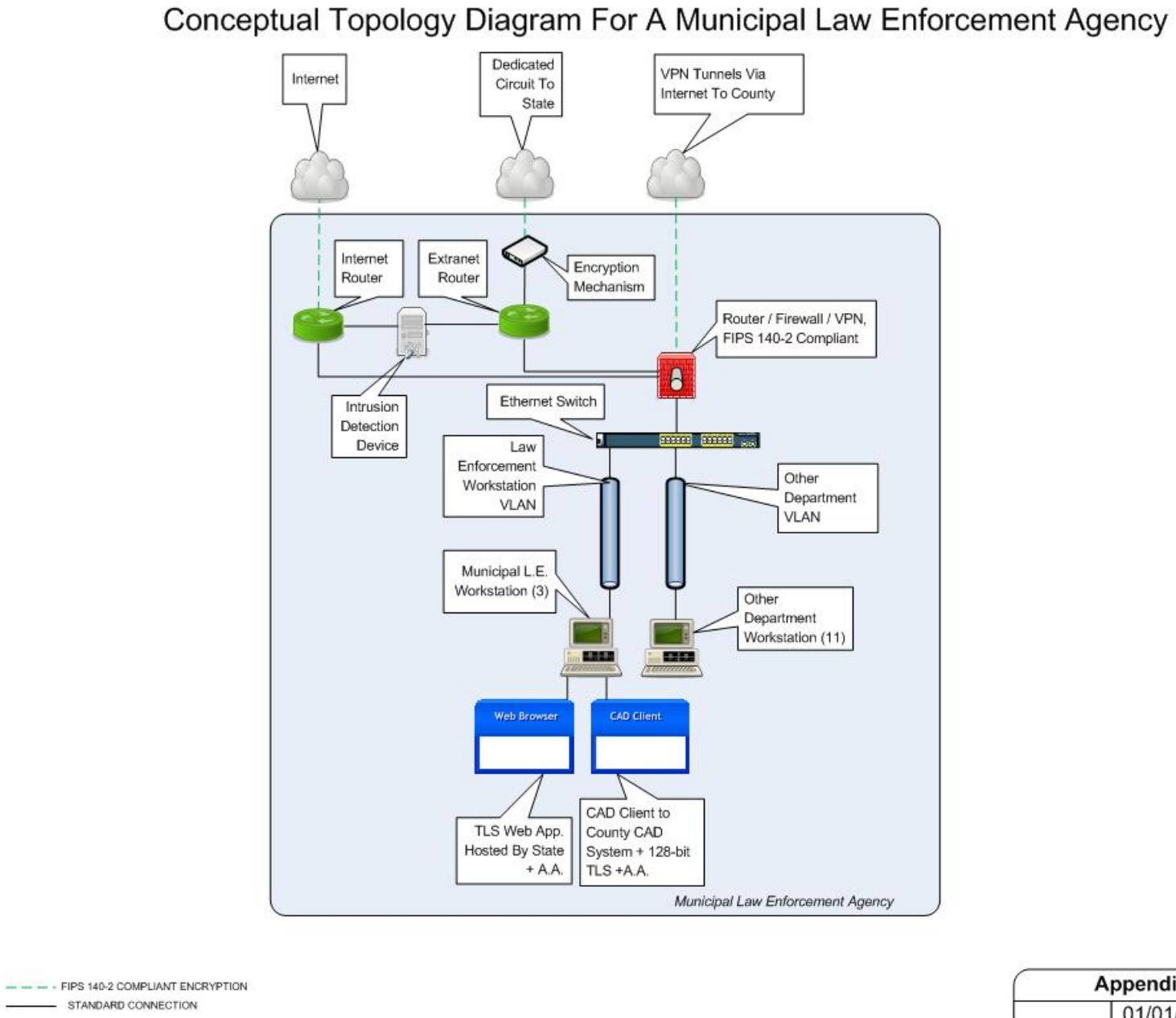
Appendix C.1-B
01/01/2011

Figure C-1-C Conceptual Topology Diagram for a County Law Enforcement Agency



Appendix C.1-C		
	01/01/2011	

Figure C-1-D Conceptual Topology Diagram for a Municipal Law Enforcement Agency



Appendix C.1-D		
	01/01/2011	

APPENDIX D SAMPLE INFORMATION EXCHANGE AGREEMENTS

D-1. CJIS User Agreement

CRIMINAL JUSTICE INFORMATION SERVICES (CJIS)

SYSTEMS USER AGREEMENT

The FBI CJIS Division provides state-of-the-art identification and information services to the local, state, tribal, federal, and international criminal justice communities, as well as the noncriminal justice community, for licensing and employment purposes. These services are administered and maintained by the FBI CJIS Division and managed in cooperation with the CJIS Systems Agency (CSA) and its administrator for CJIS data, the CJIS Systems Officer (CSO). The CJIS Systems include, but are not limited to: the Interstate Identification Index (III); National Crime Information Center (NCIC); Uniform Crime Reporting (UCR), whether summary or incident-based reporting to the National Incident-Based Reporting System; Fingerprint Identification Record System; Law Enforcement National Data Exchange (N-DEx); Law Enforcement Online; and the National Instant Criminal Background Check System (NICS).

The FBI CJIS Division provides the following services to its users, as applicable:

1. Operational, technical, and investigative assistance.

2. Telecommunication lines to state, federal, and regulatory interfaces.

3. Legal and legislative review of matters pertaining to all CJIS Systems.

4. Timely information on all aspects of all CJIS Systems and other related programs by means of operating manuals, code manuals, technical and operational updates, various newsletters, information letters, frequently asked questions, and other relevant documents.

5. Training assistance and up-to-date materials provided to each CSO, NICS Point of Contact (POC), state Compact Officer, State Administrator, Information Security Officer (ISO), and other appropriate personnel.

6. Ongoing assistance to Systems' users through meetings and briefings with the CSO**s**, State Administrators, Compact Officers, ISOs, and NICS State POCs to discuss operational and policy issues.

7. Advisory Process through which authorized users have input as to the policies and procedures governing the operation of CJIS programs.

8. National Crime Prevention and Privacy Compact Administrative Office through which states and other authorized users may submit issues concerning the noncriminal justice use of the III System.

9. Annual NICS Users Conference.

10. Audit.

11. Staff research assistance.

PART 1

The purpose behind a designated CSO is to unify responsibility for Systems user discipline and to ensure adherence to established procedures and policies within each signatory state/territory/tribal agency and by each federal user. This agreement outlines the responsibilities of each CSO as they relate to all CJIS Systems and other related CJIS administered programs. These individuals are ultimately responsible for planning necessary hardware, software, funding, and training for access to all CJIS Systems.

To ensure continued access as set forth above, the CSA agrees to adhere to all applicable CJIS policies including, but not limited to, the following:

1. The signatory state/tribal agency will provide fingerprints that meet submission criteria for all qualifying arrests. In addition, states/tribal agencies will make their records available for interstate exchange for criminal justice and other authorized purposes unless restricted by state/tribal law, and, where applicable, continue to move toward participation in the III and, upon ratification of the National Crime Prevention and Privacy Compact, the National Fingerprint File.

2. Appropriate and reasonable quality assurance procedures; e.g., hit confirmation, audits for record timeliness, and validation, must be in place to ensure that only complete, accurate, and valid information is maintained in the CJIS Systems.

3. Biannual file synchronization of information entered into the III by participating states.

4. Security - Each agency is responsible for appropriate security measures as applicable to physical security of terminals and telecommunication lines; personnel security to include background screening requirements; technical security to protect against unauthorized use; data security to include III use, dissemination, and logging; and security of criminal history records. Additionally, each CSO must ensure that all agencies establish an

information security structure that provides for an ISO and complies with the CJIS Security Policy.

5. Audit - Each agency shall be responsible for complying with all audit requirements for use of CJIS Systems. Each CSO is responsible for completing a triennial audit of all agencies with access to CJIS Systems through the CSO's lines.

6. Training - Each agency shall be responsible for training requirements, including compliance with operator training mandates.

7. Integrity of the Systems - Each agency shall be responsible for maintaining the integrity of the system in accordance with FBI CJIS Division/state/federal/tribal policies to ensure only authorized terminal access; only authorized transaction submission; and proper handling and dissemination of CJIS data. Each agency shall also be responsible for computer security incident reporting as required by the *CJIS Security Policy*.

The following documents are incorporated by reference and made part of this agreement for CSA users:

1. Bylaws for the CJIS Advisory Policy Board and Working Groups.

2. CJIS Security Policy.

3. Interstate Identification Index Operational and Technical Manual, National Fingerprint File Operations Plan, NCIC 2000 Operating Manual, UCR Handbook-NIBRS Edition, and National Incident-Based Reporting System Volumes 1, 2, and 4.

4. National Crime Prevention and Privacy Compact, 42 United States Code (U.S.C.) §14616.

5. NCIC Standards and UCR Standards, as recommended by the CJIS Advisory Policy Board.

6. The National Fingerprint File Qualification Requirements.

7. Title 28, Code of Federal Regulations, Parts 20 and 25, §50.12, and Chapter IX.

8. Electronic Fingerprint Transmission Specifications.

9. Other relevant documents, to include: NCIC Technical and Operational Updates, CJIS Information Letters, NICS User Manual, NICS Interface Control Document.

10. Applicable federal, state, and tribal laws and regulations.

PART 2

Additionally, there are authorized federal regulatory recipients and other authorized users that provide electronic fingerprint submissions through a CJIS Wide Area Network (WAN) connection (or other approved form of electronic connection) to the CJIS Division that are required to comply with the following CJIS policies:

1. The authorized user will provide fingerprints that meet submission criteria and apply appropriate and reasonable quality assurance procedures.

2. Security - Each agency is responsible for appropriate security measures as applicable to physical security of communication equipment; personnel security to include background screening requirements; technical security to protect against unauthorized use; and security of criminal history records.

3. Audit - Each authorized user shall be responsible for complying with all audit requirements for CJIS Systems. Additionally, each authorized user is subject to a triennial audit by the CJIS Division Audit staff.

4. Training - Each authorized user receiving criminal history record information shall be responsible for training requirements, including compliance with proper handling of criminal history records.

The following documents are incorporated by reference and made part of this agreement for non-CSA authorized users:

1. CJIS Security Policy.

2. National Crime Prevention and Privacy Compact, 42 U.S.C. §14616.

3. Title 28, Code of Federal Regulations, Parts 20 and 25, § 50.12, and Chapter IX.

4. Other relevant documents, to include CJIS Information Letters.

5. Applicable federal, state, and tribal laws and regulations.

GENERAL PROVISIONS

Funding:

Unless otherwise agreed in writing, each party shall bear its own costs in relation to this agreement. Expenditures will be subject to federal and state budgetary processes and availability of funds pursuant to applicable laws and regulations. The parties expressly acknowledge that this in no way implies that Congress will appropriate funds for such expenditures.

Termination:

1. All activities of the parties under this agreement will be carried out in accordance to the above-described provisions.

2. This agreement may be amended or terminated by the mutual written consent of the parties authorized representatives.

3. Either party may terminate this agreement upon 30-days written notification to the other party. Such notice will be the subject of immediate consultation by the parties to decide upon the appropriate course of action. In the event of such termination, the following rules apply:

    a. The parties will continue participation, financial or otherwise, up to the effective date of termination.

    b. Each party will pay the costs it incurs as a result of termination.

    c. All information and rights therein received under the provisions of this agreement prior to the termination will be retained by the parties, subject to the provisions of this agreement.

ACKNOWLEDGMENT AND CERTIFICATION

As a CSO or CJIS WAN Official (or other CJIS authorized official), I hereby acknowledge the duties and responsibilities as set out in this agreement. I acknowledge that these duties and responsibilities have been developed and approved by CJIS Systems users to ensure the reliability, confidentiality, completeness, and accuracy of all information contained in, or obtained by means of, the CJIS Systems. I further acknowledge that failure to comply with these duties and responsibilities may result in the imposition of sanctions against the offending state/agency; other federal, tribal, state, and local criminal justice users; and approved noncriminal justice users with System access, whether direct or indirect. The Director of the FBI (or the National Crime Prevention and Privacy Compact Council), may approve sanctions to include the termination of CJIS services.

I hereby certify that I am familiar with all applicable documents that are made part of this agreement and to all applicable federal and state laws and regulations relevant to the receipt and dissemination of documents provided through the CJIS Systems.

This agreement is a formal expression of the purpose and intent of both parties and is effective when signed. It may be amended by the deletion or modification of any provision contained therein, or by the addition of new provisions, after written concurrence of both parties. The "Acknowledgment and Certification" is being executed by the CSO or CJIS WAN Official (or other CJIS authorized official) in both an individual and representative capacity**.** Accordingly, this agreement will remain in effect after the CSO or CJIS WAN Official (or other CJIS authorized official) vacates his/her position or until it is affirmatively amended or rescinded in writing. This agreement does not confer, grant, or authorize any rights, privileges, or obligations to any third party.

SYSTEMS USER AGREEMENT

Please execute either Part 1 or Part 2

PART 1

_____ Date: _____

CJIS Systems Officer

_____

Printed Name/Title

CONCURRENCE OF CSA HEAD:

_____ Date: _____

CSA Head

_____

Printed Name/Title

PART 2

_____ Date: _____

CJIS WAN Official (or other CJIS Authorized Official)

_____

Printed Name/Title

CONCURRENCE OF CJIS WAN AGENCY HEAD:

_____ Date: _____

CJIS WAN Agency Head

_____

Printed Name/Title

FBI CJIS DIVISION:

_____ Date: _____

[Name]

Assistant Director

FBI CJIS Division

* The FBI Designated Federal Officer should be notified when a CSO or other CJIS WAN/authorized Official vacates his/her position. The name and telephone number of the Acting CSO or other CJIS WAN/authorized Official, and when known, the name and telephone number of the new CSO or other CJIS WAN/authorized Official, should be provided. Revised: 05/03/2006

D-2. Management Control Agreement

Management Control Agreement

Pursuant to the CJIS Security Policy Version 5, Sections 3.2.2 and 5.1, it is agreed that with respect to administration of that portion of computer systems and network infrastructure interfacing directly or indirectly with the state network (Network Name) for the interstate exchange of criminal history/criminal justice information, the (Criminal Justice Agency) shall have the authority, via managed control, to set and enforce:

(1) Priorities.
(2) Standards for the selection, supervision, and termination of personnel.
(3) Policy governing operation of justice systems, computers, access devices, circuits, hubs, routers, firewalls, and any other components, including encryption, that comprise and support a telecommunications network and related criminal justice systems to include but not limited to criminal history record/criminal justice information, insofar as the equipment is used to process or transmit criminal justice systems information guaranteeing the priority, integrity, and availability of service needed by the criminal justice community.
(4) Restriction of unauthorized personnel from access or use of equipment accessing the State network.
(5) Compliance with all rules and regulations of the (Criminal Justice Agency) Policies and CJIS Security Policy in the operation of all information received.

"Responsibility for management of security control shall remain with the criminal justice agency." CJIS Security Policy Version 5.0, Section 3.2.

This agreement covers the overall supervision of all (Criminal Justice Agency) systems, applications, equipment, systems design, programming, and operational procedures associated with the development, implementation, and maintenance of any (Criminal Justice Agency) system to include NCIC Programs that may be subsequently designed and/or implemented within the (Criminal Justice Agency).

_____ _____
John Smith, CIO Date
Any State Department of Administration

_____ _____
Joan Brown, CIO Date
(Criminal Justice Agency)

D-3. Noncriminal Justice Agency Agreement & Memorandum of Understanding

MEMORANDUM OF UNDERSTANDING

BETWEEN

THE FEDERAL BUREAU OF INVESTIGATION

AND

(Insert Name of Requesting Organization)

FOR

THE ESTABLISHMENT AND ACCOMMODATION OF
THIRD-PARTY CONNECTIVITY TO THE
CRIMINAL JUSTICE INFORMATION SERVICES DIVISION'S WIDE AREA NETWORK

1. PURPOSE: This Memorandum of Understanding (MOU) between the Federal Bureau of Investigation (FBI) and **(insert requesting organization's name)**, hereinafter referred to as the "parties," memorializes each party's responsibilities with regard to establishing connectivity to records services accessible via the Wide Area Network (WAN) of the FBI's Criminal Justice Information Services (CJIS) Division.

2. BACKGROUND: The requesting organization, **(insert requesting organization's name)**, being approved for access to systems of records accessible via the CJIS WAN, desires connectivity to the CJIS WAN or via a secure Virtual Private Network (VPN) Connection (Internet) to the CJIS WAN. The CJIS Division has created a framework for accommodating such requests based on the type of connection.

In preparing for such non-CJIS-funded connectivity to the CJIS WAN, the parties plan to acquire, configure, and place needed communications equipment at suitable sites and to make electronic connections to the appropriate systems of records via the CJIS WAN.

To ensure that there is a clear understanding between the parties regarding their respective roles in this process, this MOU memorializes each party's responsibilities regarding the development, operation, and maintenance of third-party connectivity to the CJIS WAN. Unless otherwise contained in an associated contract, the enclosed terms apply. If there is a conflict between terms and provisions contained in both the contract and this MOU, the contract will prevail.

3. AUTHORITY: The FBI is entering into this MOU under the authority provided by Title 28, United States Code (U.S.C.), Section 534; 42 U.S.C. § 14616; and/or Title 28, Code of Federal Regulations, Part 906.

4. SCOPE:

a. The CJIS Division agrees to:

i. Provide the requesting organization with a "CJIS WAN Third-Party Connectivity Package" that will detail connectivity requirements and options compatible with the CJIS Division's WAN architecture upon receipt of a signed nondisclosure statement.

ii. Configure the requesting organization’s connection termination equipment suite at Clarksburg, West Virginia, and prepare it for deployment or shipment under the CJIS WAN option. In the Secure VPN arrangement only, the third party will develop, configure, manage, and maintain its network connectivity to its preferred service provider.

iii. Work with the requesting organization to install the connection termination equipment suite and verify connectivity.

iv. Perform installation and/or routine maintenance on the requesting organization’s third-party dedicated CJIS WAN connection termination equipment after coordinating with the requesting organization’s designated point of contact (POC) and during a time when the CJIS Division's technical personnel are near the requesting organization’s site.

v. Perform periodic monitoring and troubleshooting of the requesting organization’s CJIS WAN connection termination equipment. Software patches will be maintained on the dedicated CJIS WAN connected network equipment only. Under the Secure VPN option, no availability or data thru-put rates will be guaranteed.

vi. Provide 24 hours a day, 7 days a week uninterrupted monitoring from the CJIS Division's Network Operations Center.

vii. Provide information regarding potential hardware end-of-life replacement cycles to the requesting organization for its budgeting purposes.

viii. Maintain third-party dedicated CJIS WAN connection termination equipment as if in the CJIS Division's operational environment.

ix. Update the appropriate software on the requesting organization's dedicated connection termination equipment connected to the CJIS WAN (i.e., Cisco Internetwork Operating System, SafeNet frame relay encryptor firmware, etc.) pursuant to the requesting organization's authorized maintenance contracts.

x. Provide a POC and telephone number for MOU-related issues.

b. The **(insert requesting organization's name)** agrees to:

i. Coordinate requests for third-party connectivity to the CJIS WAN or the Secure VPN with the CJIS Division's POC.

ii. Purchase hardware and software that are compatible with the CJIS WAN.

iii. Pay for the telecommunications infrastructure that supports its connection to the CJIS WAN or Secure VPN.

iv. Maintain telecommunication infrastructure in support of Secure VPN connectivity.

v. Provide any/all hardware and software replacements and upgrades as mutually agreed to by the parties.

vi. Pay for all telecommunication requirements related to its connectivity.

vii. Provide required information for dedicated service relating to Data Link Connection Identifiers, Circuit Identifier, Permanent Virtual Circuit Identifiers,

Local Exchange Carrier Identifier, POC, location, etc., as determined by the parties.

viii. Transport the CJIS WAN connection termination equipment suite to the CJIS Division for configuration and preparation for deployment under the dedicated service option.

ix. Provide registered Internet Protocol information to be used by the requesting organization's system to the CJIS Division.

x. Provide the CJIS Division with six months advance notice or stated amount of time for testing activities (i.e., disaster recovery exercises).

xi. Provide the CJIS Division with applicable equipment maintenance contract numbers and level of service verifications needed to perform software upgrades on connection termination equipment.

xii. Provide the CJIS Division with applicable software upgrade and patch images (or information allowing the CJIS Division to access such images).

xiii. Transport only official, authorized traffic over the Secure VPN.

xiv. Provide a POC and telephone number for MOU-related issues.

5. FUNDING: There are no reimbursable expenses associated with this level of support. Each party will fund its own activities unless otherwise agreed to in writing. This MOU is not an obligation or commitment of funds, nor a basis for transfer of funds, but rather is a basic statement of understanding between the parties hereto of the nature of the relationship for the connectivity efforts. Unless otherwise agreed to in writing, each party shall bear its own costs in relation to this MOU. Expenditures by each party will be subject to its budgetary processes and to the availability of funds and resources pursuant to applicable laws, regulations, and policies. The parties expressly acknowledge that the above language in no way implies that Congress will appropriate funds for such expenditures.

6. SETTLEMENT OF DISPUTES: Disagreements between the parties arising under or relating to this MOU will be resolved only by consultation between the parties and will not be referred to any other person or entity for settlement.

7. SECURITY: It is the intent of the parties that the actions carried out under this MOU will be conducted at the unclassified level. No classified information will be provided or generated under this MOU.

8. AMENDMENT, TERMINATION, ENTRY INTO FORCE, AND DURATION:

a. All activities of the parties under this MOU will be carried out in accordance with the above - described provisions.

b. This MOU may be amended or terminated by the mutual written consent of the parties' authorized representatives.

c. Either party may terminate this MOU upon 30-days written notification to the other party. Such notice will be the subject of immediate consultation by the parties to decide upon the appropriate course of action. In the event of such termination, the following rules apply:

i. The parties will continue participation, financial or otherwise, up to the effective date of the termination.

ii. Each party will pay the costs it incurs as a result of the termination.

iii. All information and rights therein received under the provisions of this MOU prior to the termination will be retained by the parties, subject to the provisions of this MOU.

9. FORCE AND EFFECT: This MOU, which consists of nine numbered sections, will enter into effect upon signature of the parties and will remain in effect until terminated. The parties should review the contents of this MOU annually to determine whether there is a need for the deletion, addition, or amendment of any provision. This MOU is not intended, and should not be construed, to create any right or benefit, substantive or procedural, enforceable at law or otherwise by any third party against the parties, their parent agencies, the United States, or the officers, employees, agents, or other associated personnel thereof.

The foregoing represents the understandings reached between the parties.

FOR THE FEDERAL BUREAU OF INVESTIGATION

_____ _____

[Name] Date

Assistant Director

Criminal Justice Information Services Division

FOR THE (insert requesting organization name)

_____ _____

Date

D-4. Interagency Connection Agreement

CRIMINAL JUSTICE INFORMATION SERVICES (CJIS)
Wide Area Network (WAN) USER AGREEMENT
BY INTERIM REMOTE LATENT USERS

The responsibility of the FBI CJIS Division is to provide state-of-the-art identification and information services to the local, state, federal, and international criminal justice communities, as well as the civil community for licensing and employment purposes. The data provided by the information systems administered and maintained by the FBI CJIS Division are routed to and managed in cooperation with the designated interface agency official. This information includes, but is not limited to, the Interstate Identification Index (III), National Crime Information Center (NCIC), Uniform Crime Reporting (UCR)/National Incident-Based Reporting System (NIBRS), and the Integrated Automated Fingerprint Identification System (IAFIS) programs.

In order to fulfill this responsibility, the FBI CJIS Division provides the following services to its users:

- Operational, technical, and investigative assistance;
- Telecommunications lines to local, state, federal and authorized interfaces;
- Legal and legislative review of matters pertaining to IAFIS, CJIS WAN and other related services;
- Timely information on all aspects of IAFIS, CJIS WAN, and other related programs by means of technical and operational updates, various newsletters, and other relative documents;
- Shared management through the CJIS Advisory Process and the Compact Council;
- Training assistance and up-to-date materials provided to each designated agency official, and;
- Audit.

The concept behind a designated interface agency official is to unify responsibility for system user discipline and ensure adherence to system procedures and policies within each interface agency. These individuals are ultimately responsible for planning necessary hardware, software, funding, training, and the administration of policy and procedures including security and integrity for complete access to CJIS related systems and CJIS WAN related data services by authorized agencies.

The following documents and procedures are incorporated by reference and made part of this agreement:

- *CJIS Security Policy*;
- *Title 28, Code of Federal Regulations, Part 20*;
- Computer Incident Response Capability (CIRC);
- Applicable federal and state laws and regulations.

To ensure continued access as set forth above, the designated interface agency agrees to adhere to all CJIS policies, including, but not limited to, the following:

1. The signatory criminal agency will provide fingerprints for all qualifying arrests either via electronic submission or fingerprint card that meet submission criteria. In addition, the agency will make their records available for interstate exchange for criminal justice and other authorized purposes.

2. The signatory civil agency with legislative authority will provide all qualifying fingerprints via electronic submission or fingerprint card that meet submission criteria.

3. Appropriate and reasonable quality assurance procedures must be in place to ensure that only complete, accurate, and valid information is maintained in the system.

4. Security - Each agency is responsible for appropriate security measures as applicable to physical security of terminals and telecommunications lines; Interim Distributed Imaging System (IDIS) equipment shall remain stand-

alone devices and be used only for authorized purposes; personnel security to meet background screening requirements; technical security to protect against unauthorized use; data security, dissemination, and logging for audit purposes; and actual security of criminal history records. Additionally, each agency must establish an information security structure that provides for an Information Security Officer (ISO) or a security point of contact.

5. Audit - Each agency shall be responsible for complying with the appropriate audit requirements.

6. Training - Each agency shall be responsible for training requirements, including compliance with training mandates.

7. Integrity of the system shall be in accordance with FBI CJIS Division and interface agency policies. Computer incident reporting shall be implemented.

Until states are able to provide remote latent connectivity to their respective latent communities via a state WAN connection, the CJIS Division may provide direct connectivity to IAFIS via a dial-up connection or through the Combined DNA Index System (CODIS) and/or National Integrated Ballistics Information Network (NIBIN) connections. When a state implements a latent management system and is able to provide intrastate connectivity and subsequent forwarding to IAFIS, this agreement may be terminated. Such termination notice will be provided in writing by either the FBI or the state CJIS Systems Agency.

It is the responsibility of the local remote latent user to develop or acquire an IAFIS compatible workstation. These workstations may use the software provided by the FBI or develop their own software, provided it is IAFIS compliant.

The CJIS Division will provide the approved modem and encryptors required for each dial-up connection to IAFIS. The CJIS Communication Technologies Unit will configure and test the encryptors before they are provided to the user. Users requesting remote latent connectivity through an existing CODIS and/or NIBIN connection must receive verification from the FBI that there are a sufficient number of Ethernet ports on the router to accommodate the request.

If at any time search limits are imposed by the CJIS Division, these individual agency connections will be counted toward the total state allotment.

ACKNOWLEDGMENT AND CERTIFICATION

As a CJIS WAN interface agency official serving in the CJIS system, I hereby acknowledge the duties and responsibilities as set out in this agreement. I acknowledge that these duties and responsibilities have been developed and approved by CJIS system users in order to ensure the reliability, confidentiality, completeness, and accuracy of all information contained in or obtained by means of the CJIS system. I further acknowledge that a failure to comply with these duties and responsibilities may subject our agency to various sanctions adopted by the CJIS Advisory Policy Board and approved by the Director of the FBI. These sanctions may include the termination of CJIS service.

As the designated CJIS WAN interface agency official serving in the CJIS system, I hereby certify that I am familiar with the contents of the *Title 28, Code of Federal Regulations, Part 20; CJIS Security Policy; Computer Incident Response Capability;* and applicable federal or state laws and regulations applied to IAFIS and CJIS WAN Programs for the dissemination of criminal history records for criminal and noncriminal justice purposes.

*_____ _____

Signature Print or Type

CJIS WAN Agency Official Date

CONCURRENCE OF FEDERAL/REGULATORY AGENCY HEAD OR STATE CJIS SYSTEMS OFFICER (CSO):

*_____ _____

Signature Print or Type

*_____ _____

Title Date

State CSO

FBI CJIS DIVISION:

_____

Signature – [Name]

Assistant Director _____

Title Date

* If there is a change in the CJIS WAN interface agency official, the FBI Designated Federal Employee must be notified in writing 30 days prior to the change.

5/27/2004 UA modification reflects change in CTO title to CSO.

APPENDIX E SECURITY FORUMS AND ORGANIZATIONAL ENTITIES

Online Security Forums / Organizational Entities
AntiOnline
Black Hat
CIO.com
CSO Online
CyberSpeak Podcast
FBI Criminal Justice Information Services Division (CJIS)
Forrester Security Forum
Forum of Incident Response and Security Teams (FIRST)
Information Security Forum (ISF)
Information Systems Audit and Control Association (ISACA)
Information Systems Security Association (ISSA)
Infosyssec
International Organization for Standardization (ISO)
International Information Systems Security Certification Consortium, Inc. $(ISC)^2$
Metasploit
Microsoft Developer Network (MSDN) Information Security
National Institute of Standards and Technology (NIST)
Open Web Application Security Project (OWASP)
SANS (SysAdmin, Audit, Network, Security) Institute
SC Magazine
Schneier.com
Security Focus
The Register
US Computer Emergency Response Team (CERT)
US DoJ Computer Crime and Intellectual Property Section (CCIPS)

APPENDIX F IT SECURITY INCIDENT RESPONSE FORM

FBI CJIS DIVISION

INFORMATION SECURITY OFFICER (ISO)

***COMPUTER SECURITY INCIDENT RESPONSE CAPABILITY* (CSIRC)**

REPORTING FORM

DATE OF REPORT: _____ (mm/dd/yyyy)

DATE OF INCIDENT: _____ (mm/dd/yyyy)

POINT(S) OF CONTACT: _____ PHONE/EXT/E-MAIL: _____

LOCATION(S) OF INCIDENT: _____

SYSTEM(S) AFFECTED: _____

_____

METHOD OF DETECTION: _____

NATURE OF INCIDENT: _____

_____

INCIDENT DESCRIPTION: _____

_____

ACTIONS TAKEN/RESOLUTION: _____

_____

_____

Copies To:

George White
(FBI CJIS Division ISO)
1000 Custer Hollow Road
Clarksburg, WV 26306-0102
(304) 625-5849
george.white@leo.gov
or
iso@leo.gov

George White
(FBI CJIS CSIRC POC)
1000 Custer Hollow Road/Module D-2
Clarksburg, WV 26306-0102
(304) 625-5849
george.white@leo.gov
or
iso@leo.gov

APPENDIX G BEST PRACTICES

G-1. Virtualization

Virtualization

This appendix documents security considerations for implementing and operating virtual environments that process, store, and/or transmit Criminal Justice Information.

The FBI CJIS ISO has fielded several inquiries from various states requesting guidance on implementing virtual environments within their data centers. With the proliferation of virtual environments across industry in general there is a realistic expectation that FBI CJIS Auditors will encounter virtual environments during the upcoming year. Criminal Justice Agencies (CJAs) and Noncriminal Justice Agencies (NCJAs) alike need to understand and appreciate the foundation of security protection measures required for virtual environments.

From Microsoft's Introduction to Windows Server 2008
http://www.microsoft.com/windowsserver2008/en/us/hyperv.aspx:

> *"Server virtualization, also known as hardware virtualization, is a hot topic in the IT world because of the potential for serious economic benefits. Server virtualization enables multiple operating systems to run on a single physical machine as virtual machines (VMs). With server virtualization, you can consolidate workloads across multiple underutilized server machines onto a smaller number of machines. Fewer physical machines can lead to reduced costs through lower hardware, energy, and management overhead, plus the creation of a more dynamic IT infrastructure."*

From a trade publication, kernelthread.com
http://www.kernelthread.com/publications/virtualization/:

> *"Virtualization is a framework or methodology of dividing the resources of a computer into multiple execution environments, by applying one or more concepts or technologies such as hardware and software partitioning, time-sharing, partial or complete machine simulation, emulation, quality of service, and many others."*

From an Open Source Software developer
http://www.kallasoft.com/pc-hardware-virtualization-basics/:

> *"Virtualization refers to virtualizing hardware in software, allowing multiple operating systems, or images, to run concurrently on the same hardware. There are two main types of virtualization software:*
>
> - *"Type-1 Hypervisor, which runs 'bare-metal' (on top of the hardware)*
> - *"Type-2 Hypervisor which requires a separate application to run within an operating system*
>
> *"Type1 hypervisors usually offer the best in efficiency, while Type-2 hypervisors allow for greater support of hardware that can be provided by the operating*

system. For the developer, power user, and small business IT professionals, virtualization offers the same basic idea of collapsing multiple physical boxes into one. For instance, a small business can run a web server and an Exchange server without the need for two boxes. Developers and power users can use the ability to contain different development environments without the need to modify their main operating system. Big businesses can also benefit from virtualization by allowing software maintenance to be run and tested on a separate image on hardware without having to take down the main production system."

Industry leaders and niche developers are bringing more products to market every day. The following article excerpts, all posted during September 2008, on www.virtualization.com are examples of industry offerings.

"Microsoft and Novell partnered together for joint virtualization solution. Microsoft and Novell are announcing the availability of a joint virtualization solution optimized for customers running mixed-source environments. The joint offering includes SUSE Linux Enterprise Server configured and tested as an optimized guest operating system running on Windows Sever 2008 Hyper-V, and is fully support by both companies' channel partners. The offering provides customers with the first complete, fully supported and optimized virtualization solution to span Windows and Linux environments."

"Sun Microsystems today account the availability of Sun xVM Server software and Sun xVM Ops Center 2.0, key components in its strategy. Sun also announced the addition of comprehensive services and support for Sun xVM Server software and xVM Ops Center 2.0 to its virtualization suite of services. Additionally, Sun launched xVMserver.org, a new open source community, where developers can download the first source code bundle for SunxVM Server software and contribute to the direction and development of the product."

"NetEx, specialist in high-speed data transport over TCP, today announced Vistual HyperIP bandwidth optimization solutions for VMware environments that deliver a threefold to tenfold increase in data replication performance. Virtual HyperIP is a software-based Data Transport Optimizer that operates on the VMware ESX server and boosts the performance of storage replication applications from vendors such as EMC, NetApp, Symantec, IBM, Data Domain, and FalconStor. Virtual HyperIP mitigates TCP performance issues that are common when moving data over wide –area network (WAN) connections because of bandwidth restrictions, latency due to distance and/or router hop counts, packet loss and network errors. Like the company's award-winning appliance-based HyperIP, Virtual HyperIP eliminates these issues with an innovative software design developed specifically to accelerate traffic over an IP based network."

From several sources, particularly:

http://www.windowsecurity.com/articles/security-virutalization.html
http://csrc.nist.gov/publications/drafts/6--=64rev2/draft-sp800-64-Revision2.pdf

Virtualization provides several benefits:

- Make better use of under-utilized servers by consolidating to fewer machines saving on hardware, environmental costs, management, and administration of the server infrastructure.
- Legacy applications unable to run on newer hardware and/or operating systems can be loaded into a virtual environment – replicating the legacy environment.
- Provides for isolated portions of a server where trusted and untrusted applications can be ran simultaneously – enabling hot standbys for failover.
- Enables existing operating systems to run on shared memory multiprocessors.
- System migration, backup, and recovery are easier and more manageable.

Virtualization also introduces several vulnerabilities:

- Host Dependent.
- If the host machine has a problem then all the VMs could potentially terminate.
- Compromise of the host makes it possible to take down the client servers hosted on the primary host machine.
- If the virtual network is compromised then the client is also compromised.
- Client share and host share can be exploited on both instances. Potentially this can lead to files being copied to the share that fill up the drive.

These vulnerabilities can be mitigated by the following factors:

- Apply "least privilege" technique to reduce the attack surface area of the virtual environment and access to the physical environment.
- Configuration and patch management of the virtual machine and host, i.e. Keep operating systems and application patches up to date on both virtual machines and hosts.
- Install the minimum applications needed on host machines.
- Practice isolation from host and virtual machine.
- Install and keep updated antivirus on virtual machines and the host.
- Segregation of administrative duties for host and versions.
- Audit logging as well as exporting and storing the logs outside the virtual environment.
- Encrypting network traffic between the virtual machine and host IDS and IPS monitoring.
- Firewall each virtual machine from each other and ensure that only allowed protocols will transact.

Security Policy Working Group (SPWG) White Paper:

Voice over Internet Protocol (VoIP)

Attribution:

The following information has been extracted from NIST Special Publication 800-58, Security Considerations for Voice over IP Systems.

Definitions:

Voice over Internet Protocol (VoIP) – A set of software, hardware, and standards designed to make it possible to transmit voice over packet switched networks, either an internal Local Area Network, or across the Internet.

Internet Protocol (IP) - A protocol used for communicating data across a packet-switched internetwork using the Internet Protocol Suite, also referred to as TCP/IP. IP is the primary protocol in the Internet Layer of the Internet Protocol Suite and has the task of delivering distinguished protocol datagrams (packets) from the source host to the destination host solely based on their addresses.

Summary:

Voice over Internet Protocol (VoIP) has been embraced by organizations globally as an addition to, or replacement for, public switched telephone network (PSTN) and private branch exchange (PBX) telephone systems. The immediate benefits are alluring since the typical cost to operate VoIP is less than traditional telephone services and VoIP can be installed in-line with an organization's existing Internet Protocol services. Unfortunately, installing a VoIP network is not a simple "plug-and-play" procedure. There are myriad security concerns, cost issues with new networking hardware requirements, and overarching quality of service (QoS) factors that have to be considered carefully.

What are some of the advantages of VoIP?

a. Cost – a VoIP system is usually cheaper to operate than an equivalent office telephone system with a Private Branch Exchange and conventional telephone service.

b. Integration with other services – innovative services are emerging that allow customers to combine web access with telephone features through a single PC or terminal. For example, a sales representative could discuss products with a customer

using the company's web site. In addition, the VoIP system may be integrated with video across the Internet, providing a teleconferencing facility.

What are some of the disadvantages of VoIP?

a. Startup cost – although VoIP can be expected to save money in the long run, the initial installation can be complex and expensive. In addition, a single standard has not yet emerged for many aspects of VoIP, so an organization must plan to support more than one standard, or expect to make relatively frequent changes as the VoIP field develops.

b. Security – the flexibility of VoIP comes at a price: added complexity in securing voice and data. Because VoIP systems are connected to the data network, and share many of the same hardware and software components, there are more ways for intruders to attack a VoIP system than a conventional voice telephone system or PBX.

VoIP Risks, Threats, and Vulnerabilities

This section details some of the potential threats and vulnerabilities in a VoIP environment, including vulnerabilities of both VoIP phones and switches. Threat discussion is included because the varieties of threats faced by an organization determine the priorities in securing its communications equipment. Not all threats are present in all organizations. A commercial firm may be concerned primarily with toll fraud, while a government agency may need to prevent disclosure of sensitive information because of privacy or national security concerns. Information security risks can be broadly categorized into the following three types: confidentiality, integrity, and availability, (which can be remembered with the mnemonic "CIA"). Additional risks relevant to switches are fraud and risk of physical damage to the switch, physical network, or telephone extensions.

Packet networks depend for their successful operation on a large number of configurable parameters: IP and MAC (physical) addresses of voice terminals, addresses of routers and firewalls, and VoIP specific software such as Call Managers and other programs used to place and route calls. Many of these network parameters are established dynamically every time a network component is restarted, or when a VoIP telephone is restarted or added to the network. Because there are so many places in a network with dynamically configurable parameters, intruders have a wide array of potentially vulnerable points to attack.

Vulnerabilities described in this section are generic and may not apply to all systems, but investigations by NIST and other organizations have found these vulnerabilities in a number of VoIP systems. In addition, this list is not exhaustive; systems may have security weaknesses that are not included in the list. For each potential vulnerability, a recommendation is included to eliminate or reduce the risk of compromise.

Confidentiality and Privacy

Confidentiality refers to the need to keep information secure and private. For home computer users, this category includes confidential memoranda, financial information, and security information such as passwords. In a telecommunications switch,

eavesdropping on conversations is an obvious concern, but the confidentiality of other information on the switch must be protected to defend against toll fraud, voice and data interception, and denial of service attacks. Network IP addresses, operating system type, telephone extension to IP address mappings, and communication protocols are all examples of information that, while not critical as individual pieces of data, can make an attacker's job easier

With conventional telephones, eavesdropping usually requires either physical access to tap a line, or penetration of a switch. Attempting physical access increases the intruder's risk of being discovered, and conventional PBXs have fewer points of access than VoIP systems. With VoIP, opportunities for eavesdroppers increase dramatically, because of the many nodes in a packet network.

Switch Default Password Vulnerability

It is common for switches to have a default login/password set, e.g., admin/admin, or root /root. This vulnerability also allows for wiretapping conversations on the network with port mirroring or bridging. An attacker with access to the switch administrative interface can mirror all packets on one port to another, allowing the indirect and unnoticeable interception of all communications. Failing to change default passwords is one of the most common errors made by inexperienced users.

REMEDIATION: If possible, remote access to the graphical user interface should be disabled to prevent the interception of plaintext administration sessions. Some devices provide the option of a direct USB connection in addition to remote access through a web browser interface. Disabling port mirroring on the switch should also be considered.

Classical Wiretap Vulnerability

Attaching a packet capture tool or protocol analyzer to the VoIP network segment makes it easy to intercept voice traffic.

REMEDIATION: A good physical security policy for the deployment environment is a general first step to maintaining confidentiality. Disabling the hubs on IP Phones as well as developing an alarm system for notifying the administrator when an IP Phone has been disconnected will allow for the possible detection of this kind of attack.

ARP Cache Poisoning and ARP Floods

Because many systems have little authentication, an intruder may be able to log onto a computer on the VoIP network segment, and then send ARP commands corrupting ARP caches on sender(s) of desired traffic, then activate IP. An ARP flood attack on the switch could render the network vulnerable to conversation eavesdropping. Broadcasting ARP replies blind is sufficient to corrupt many ARP caches. Corrupting the ARP cache makes it possible to re-route traffic to intercept voice and data traffic.

REMEDIATION: Use authentication mechanisms wherever possible and limit physical access to the VoIP network segment.

Web Server interfaces

Both VoIP switches and voice terminals are likely to have a web server interface for remote or local administration. An attacker may be able to sniff plaintext HTTP packets to gain confidential information. This would require access to the local network on which the server resides.

REMEDIATION: If possible, do not use an HTTP server. If it is necessary to use a web server for remote administration, use the more secure HTTPS (HTTP over SSL or TLS) protocol.

IP Phone Netmask Vulnerability

A similar effect of the ARP Cache Vulnerability can be achieved by assigning a subnet mask and router address to the phone crafted to cause most or all of the packets it transmits to be sent to an attacker's MAC address. Again, standard IP forwarding makes the intrusion all but undetectable.

REMEDIATION: A firewall filtering mechanism can reduce the probability of this attack. Remote access to IP phones is a severe risk.

Extension to IP Address Mapping Vulnerability

Discovering the IP address corresponding to any extension requires only calling that extension and getting an answer. A protocol analyzer or packet capture tool attached to the hub on the dialing instrument will see packets directly from the target instrument once the call is answered. Knowing the IP address of a particular extension is not a compromise in itself, but makes it easier to accomplish other attacks. For example, if the attacker is able to sniff packets on the local network used by the switch, it will be easy to pick out packets sent and received by a target phone. Without knowledge of the IP address of the target phone, the attacker's job may be much more difficult to accomplish and require much longer, possibly resulting in the attack being discovered.

REMEDIATION: Disabling the hub on the IP Phone will prevent this kind of attack. However, it is a rather simple task to turn the hub back on.

Integrity Issues

Integrity of information means that information remains unaltered by unauthorized users. For example, most users want to ensure that bank account numbers cannot be changed by anyone else, or that passwords are changed only by the user or an authorized security administrator. Telecommunication switches must protect the integrity of their system data and configuration. Because of the richness of feature sets available on switches, an attacker who can compromise the system configuration can accomplish nearly any other goal. For example, an ordinary extension could be re-assigned into a pool of phones that supervisors can listen in on or record conversations for quality control purposes. Damaging or deleting information about the IP network used by a VoIP switch results in an immediate denial of service.

The security system itself provides the capabilities for system abuse and misuse. That is, compromise of the security system not only allows system abuse but also allows the elimination of all traceability and the insertion of trapdoors for intruders to use on their

next visit. For this reason, the security system must be carefully protected. Integrity threats include any in which system functions or data may be corrupted, either accidentally or as a result of malicious actions. Misuse may involve legitimate users (i.e. insiders performing unauthorized operations) or intruders.

A legitimate user may perform an incorrect, or unauthorized, operations function (e.g., by mistake or out of malice) and may cause deleterious modification, destruction, deletion, or disclosure of switch software and data. This threat may be caused by several factors including the possibility that the level of access permission granted to the user is higher than what the user needs to remain functional.

Intrusion - An intruder may masquerade as a legitimate user and access an operations port of the switch. There are a number of serious intrusion threats. For example, the intruder may use the permission level of the legitimate user and perform damaging operations functions such as:

- Disclosing confidential data
- Causing service deterioration by modifying the switch software
- Crashing the switch
- Removing all traces of the intrusion (e.g., modifying the security log) so that it may not be readily detected

Insecure state - At certain times the switch may be vulnerable due to the fact that it is not in a secure state. For example:

- After a system restart, the old security features may have been reset to insecure settings, and new features may not yet be activated. (For example, all old passwords may have reverted to the default system-password, even though new passwords are not yet assigned.) The same may happen at the time of a disaster recovery.
- At the time of installation the switch may be vulnerable until the default security features have been replaced.

DHCP Server Insertion Attack

It is often possible to change the configuration of a target phone by exploiting the DHCP response race when the IP phone boots. As soon as the IP phone requests a DHCP response, a rogue DHCP server can initiate a response with data fields containing false information.

This attack allows for possible man in the middle attacks on the IP-media gateway, and IP Phones. Many methods exist with the potential to reboot the phone remotely, e.g. “social engineering”, ping flood, MAC spoofing (probably SNMP hooks, etc.).

REMEDIATION: If possible, use static IP addresses for the IP Phones. This will remove the necessity of using a DHCP server. Further, using a state based intrusion detection system can filter out DHCP server packets from IP Phone ports, allowing this traffic only from the legitimate server.

TFTP Server Insertion Attack

It is possible to change the configuration of a target phone by exploiting the TFTP response race when the IP phone is resetting. A rogue TFTP server can supply spurious information before the legitimate server is able to respond to a request. This attack allows an attacker to change the configuration of an IP Phone.

REMEDIATION: Using a state based intrusion detection system can filter out DHCP server packets from IP Phone ports, allowing such traffic only from the legitimate server. Organizations looking to deploy VoIP systems should look for IP Phone instruments that can download signed binary files.

Availability and Denial of Service

Availability refers to the notion that information and services be available for use when needed. Availability is the most obvious risk for a switch. Attacks exploiting vulnerabilities in the switch software or protocols may lead to deterioration or even denial of service or functionality of the switch. For example: if unauthorized access can be established to any branch of the communication channel (such as a CCS link or a TCP/IP link), it may be possible to flood the link with bogus messages causing severe deterioration (possibly denial) of service. A voice over IP system may have additional vulnerabilities with Internet connections. Because intrusion detection systems fail to intercept a significant percentage of Internet based attacks, attackers may be able to bring down VoIP systems by exploiting weaknesses in Internet protocols and services.

Any network may be vulnerable to denial of service attacks, simply by overloading the capacity of the system. With VoIP the problem may be especially severe, because of its sensitivity to packet loss or delay.

CPU Resource Consumption Attack without any account information.

An attacker with remote terminal access to the server may be able to force a system restart (shutdown all/restart all) by providing the maximum number of characters for the login and password buffers multiple times in succession. Additionally, IP Phones may reboot as a result of this attack.

In addition to producing a system outage, the restart may not restore uncommitted changes or, in some cases, may restore default passwords, which would introduce intrusion vulnerabilities.

REMEDIATION: The deployment of a firewall disallowing connections from unnecessary or unknown network entities is the first step to overcoming this problem. However, there is still the opportunity for an attacker to spoof his MAC and IP address, circumventing the firewall protection.

Default Password Vulnerability

It is common for switches to have a default login/password set, e.g., admin/admin, or root /root. Similarly, VoIP telephones often have default keypad sequences that can be used to unlock and modify network information

This vulnerability would allow an attacker to control the topology of the network remotely, allowing for not only complete denial of service to the network, but also a port mirroring attack to the attacker's location, giving the ability to intercept any other conversations taking place over the same switch. Further, the switch may have a web server interface, providing an attacker with the ability to disrupt the network without advance knowledge of switch operations and commands. In most systems, telephones download their configuration data on startup using TFTP or similar protocols. The configuration specifies the IP addresses for Call Manager nodes, so an attacker could substitute another IP address pointing to a call manager that would allow eavesdropping or traffic analysis.

REMEDIATION: Changing the default password is crucial. Moreover, the graphical user interface should be disabled to prevent the interception of plaintext administration sessions.

Exploitable software flaws

Like other types of software, VoIP systems have been found to have vulnerabilities due to buffer overflows and improper packet header handling. These flaws typically occur because the software is not validating critical information properly. For example, a short integer may be used as a table index without checking whether the parameter passed to the function exceeds 32,767, resulting in invalid memory accesses or crashing of the system.

Exploitable software flaws typically result in two types of vulnerabilities: denial of service or revelation of critical system parameters. Denial of service can often be implemented remotely, by passing packets with specially constructed headers that cause the software to fail. In some cases the system can be crashed, producing a memory dump in which an intruder can find IP addresses of critical system nodes, passwords, or other security-relevant information. In addition, buffer overflows that allow the introduction of malicious code have been found in VoIP software, as in other applications.

REMEDIATION: These problems require action from the software vendor, and distribution of patches to administrators. Intruders monitor announcements of vulnerabilities, knowing that many organizations require days or weeks to update their software. Regular checking for software updates and patches is essential to reducing these vulnerabilities. Automated patch handling can assist in reducing the window of opportunity for intruders to exploit known software vulnerabilities.

Account Lockout Vulnerability

An attacker will be able to provide several incorrect login attempts at the telnet prompt until the account becomes locked out. (This problem is common to most password-protected systems, because it prevents attackers from repeating login attempts until the correct password is found by trying all possible combinations.)

The account is unable to connect to the machine for the set lockout time.

REMEDIATION: If remote access is not available, this problem can be solved with physical access control.

NIST Recommendations.

Because of the integration of voice and data in a single network, establishing a secure VoIP and data network is a complex process that requires greater effort than that required for data-only networks. In particular, start with these general guidelines, recognizing that practical considerations, such as cost or legal requirements, may require adjustments for the organization:

1. Develop appropriate network architecture.

- Separate voice and data on logically different networks if feasible. Different subnets with separate RFC 1918 address blocks should be used for voice and data traffic, with separate DHCP servers for each, to ease the incorporation of intrusion detection and VoIP firewall protection at the voice gateway, which interfaces with the PSTN, disallow H.323, SIP, or other VoIP protocols from the data network. Use strong authentication and access control on the voice gateway system, as with any other critical network component. Strong authentication of clients towards a gateway often presents difficulties, particularly in key management. Here, access control mechanisms and policy enforcement may help.

- A mechanism to allow VoIP traffic through firewalls is required. There are a variety of protocol dependent and independent solutions, including application level gateways (ALGs) for VoIP protocols, Session Border Controllers, or other standards-based solutions when they mature.

- Stateful packet filters can track the state of connections, denying packets that are not part of a properly originated call. (This may not be practical when multimedia protocol inherent security or lower layer security is applied, e.g., H.235 Annex D for integrity provision or TLS to protect SIP signaling.)

- Use IPsec or Secure Shell (SSH) for all remote management and auditing access. If practical, avoid using remote management at all and do IP PBX access from a physically secure system.

- If performance is a problem, use encryption at the router or other gateway, not the individual endpoints, to provide for IPsec tunneling. Since some VoIP endpoints are not computationally powerful enough to perform encryption, placing this burden at a central point ensures all VoIP traffic emanating from the enterprise network has been encrypted. Newer IP phones are able to provide Advanced Encryption System (AES) encryption at reasonable cost. Note that Federal Information Processing Standard (FIPS) 140-2, Security Requirements for Cryptographic Modules, is applicable to all Federal agencies that use

cryptographic-based security systems to protect sensitive information in computer and telecommunication systems (including voice systems) as defined in Section 5131 of the Information Technology Management Reform Act of 1996, Public Law 104-106.

2. Ensure that the organization has examined and can acceptably manage and mitigate the risks to their information, system operations, and continuity of essential operations when deploying VoIP systems.

VoIP can provide more flexible service at lower cost, but there are significant tradeoffs that must be considered. VoIP systems can be expected to be more vulnerable than conventional telephone systems, in part because they are tied in to the data network, resulting in additional security weaknesses and avenues of attack (see VoIP Risks, Threats, and Vulnerabilities section for more detailed discussion of vulnerabilities of VoIP and their relation to data network vulnerabilities).

Confidentiality and privacy may be at greater risk in VoIP systems unless strong controls are implemented and maintained. An additional concern is the relative instability of VoIP technology compared with established telephony systems. Today, VoIP systems are still maturing and dominant standards have not emerged. This instability is compounded by VoIP's reliance on packet networks as a transport medium. The public switched telephone network is ultra-reliable. Internet service is generally much less reliable, and VoIP cannot function without Internet connections, except in the case of large corporate or other users who may operate a private network. Essential telephone services, unless carefully planned, deployed, and maintained, will be at greater risk if based on VoIP.

3. Special consideration should be given to E-911 emergency services communications, because E-911 automatic location service is not available with VoIP in some cases.

Unlike traditional telephone connections, which are tied to a physical location, VoIP's packet switched technology allows a particular number to be anywhere. This is convenient for users, because calls can be automatically forwarded to their locations. But the tradeoff is that this flexibility severely complicates the provision of E-911 service, which normally provides the caller's location to the 911 dispatch office. Although most VoIP vendors have workable solutions for E-911 service, government regulators and vendors are still working out standards and procedures for 911 services in a VoIP environment. Agencies must carefully evaluate E-911 issues in planning for VoIP deployment.

4. Agencies should be aware that physical controls are especially important in a VoIP environment and deploy them accordingly.

Unless the VoIP network is encrypted, anyone with physical access to the office LAN could potentially connect network monitoring tools and tap into telephone conversations. Although conventional telephone lines can also be monitored when physical access is obtained, in most offices there are many more points to connect with a LAN without arousing suspicion. Even if encryption is used, physical access to VoIP servers and gateways may allow an attacker to do traffic analysis (i.e., determine which parties are communicating). Agencies therefore should ensure that adequate physical security is in place to restrict access to VoIP network components. Physical securities measures,

including barriers, locks, access control systems, and guards, are the first line of defense. Agencies must make sure that the proper physical countermeasures are in place to mitigate some of the biggest risks such as insertion of sniffers or other network monitoring devices. Otherwise, practically speaking this means that installation of a sniffer could result in not just data but all voice communications being intercepted.

5. VoIP-ready firewalls and other appropriate protection mechanisms should be employed. Agencies must enable, use, and routinely test the security features that are included in VoIP systems.

Because of the inherent vulnerabilities (e.g. susceptibility to packet sniffing) when operating telephony across a packet network, VoIP systems incorporate an array of security features and protocols. Organization security policy should ensure that these features are used. In particular, firewalls designed for VoIP protocols are an essential component of a secure VoIP system.

6. If practical, "softphone" systems, which implement VoIP using an ordinary PC with a headset and special software, should not be used where security or privacy are a concern.

Worms, viruses, and other malicious software are extraordinarily common on PCs connected to the internet, and very difficult to defend against. Well-known vulnerabilities in web browsers make it possible for attackers to download malicious software without a user's knowledge, even if the user does nothing more than visit a compromised web site. Malicious software attached to email messages can also be installed without the user's knowledge, in some cases even if the user does not open the attachment. These vulnerabilities result in unacceptably high risks in the use of "softphones", for most applications. In addition, because PCs are necessarily on the data network, using a softphone system conflicts with the need to separate voice and data networks to the greatest extent practical.

7. If mobile units are to be integrated with the VoIP system, use products implementing WiFi Protected Access (WPA), rather than 802.11 Wired Equivalent Privacy (WEP).

The security features of 802.11 WEP provide little or no protection because WEP can be cracked with publicly available software. The more recent WiFi Protected Access (WPA), a snapshot of the ongoing 802.11i standard, offers significant improvements in security, and can aid the integration of wireless technology with VoIP. NIST strongly recommends that the WPA (or WEP if WPA is unavailable) security features be used as part of an overall defense-in-depth strategy. Despite their weaknesses, the 802.11 security mechanisms can provide a degree of protection against unauthorized disclosure, unauthorized network access, or other active probing attacks. However, the Federal Information Processing Standard (FIPS) 140-2, Security Requirements for Cryptographic Modules, is mandatory and binding for Federal agencies that have determined that certain information must be protected via cryptographic means. As currently defined, neither WEP nor WPA meets the FIPS 140-2 standard. In these cases, it will be necessary to employ higher level cryptographic protocols and applications such as secure shell (SSH), Transport Level Security (TLS) or Internet Protocol Security (IPsec) with FIPS 140-2 validated cryptographic modules and associated algorithms to protect information, regardless of whether the nonvalidated data link security protocols are used.

8. Carefully review statutory requirements regarding privacy and record retention with competent legal advisors.

Although legal issues regarding VoIP are beyond the scope of this document, readers should be aware that laws and rulings governing interception or monitoring of VoIP lines, and retention of call records, may be different from those for conventional telephone systems. Agencies should review these issues with their legal advisors. See Section 2.5 for more on these issues.

APPENDIX H SECURITY ADDENDUM

The following pages contain the legal authority, purpose, and genesis of the Criminal Justice Information Services Security Addendum (H2-H4); the Security Addendum itself (H5-H6); and the Security Addendum Certification page (H7).

FEDERAL BUREAU OF INVESTIGATION
CRIMINAL JUSTICE INFORMATION SERVICES
SECURITY ADDENDUM

Legal Authority for and Purpose and Genesis of the Security Addendum

Traditionally, law enforcement and other criminal justice agencies have been responsible for the confidentiality of their information. Accordingly, until mid-1999, the Code of Federal Regulations Title 28, Part 20, subpart C, and the National Crime Information Center (NCIC) policy paper approved December 6, 1982, required that the management and exchange of criminal justice information be performed by a criminal justice agency or, in certain circumstances, by a noncriminal justice agency under the management control of a criminal justice agency.

In light of the increasing desire of governmental agencies to contract with private entities to perform administration of criminal justice functions, the FBI sought and obtained approval from the United States Department of Justice (DOJ) to permit such privatization of traditional law enforcement functions under certain controlled circumstances. In the Federal Register of May 10, 1999, the FBI published a Notice of Proposed Rulemaking, announcing as follows:

> 1. Access to CHRI [Criminal History Record Information] and Related Information, Subject to Appropriate Controls, by a Private Contractor Pursuant to a Specific Agreement with an Authorized Governmental Agency To Perform an Administration of Criminal Justice Function (Privatization). Section 534 of title 28 of the United States Code authorizes the Attorney General to exchange identification, criminal identification, crime, and other records for the official use of authorized officials of the federal government, the states, cities, and penal and other institutions. This statute also provides, however, that such exchanges are subject to cancellation if dissemination is made outside the receiving departments or related agencies. Agencies authorized access to CHRI traditionally have been hesitant to disclose that information, even in furtherance of authorized criminal justice functions, to anyone other than actual agency employees lest such disclosure be viewed as unauthorized. In recent years, however, governmental agencies seeking greater efficiency and economy have become increasingly interested in obtaining support services for the administration of criminal justice from the private sector. With the concurrence of the FBI's Criminal Justice Information Services (CJIS) Advisory Policy Board, the DOJ has concluded that disclosures to private persons and entities providing support services for criminal justice agencies may, when subject to appropriate controls, properly be viewed as permissible disclosures for purposes of compliance with 28 U.S.C. 534.
>
> We are therefore proposing to revise 28 CFR 20.33(a)(7) to provide express authority for such arrangements. The proposed authority is similar to the authority that already exists in 28 CFR 20.21(b)(3) for state and local CHRI systems. Provision of CHRI under this authority would only be permitted pursuant to a specific agreement with an authorized governmental

agency for the purpose of providing services for the administration of criminal justice. The agreement would be required to incorporate a security addendum approved by the Director of the FBI (acting for the Attorney General). The security addendum would specifically authorize access to CHRI, limit the use of the information to the specific purposes for which it is being provided, ensure the security and confidentiality of the information consistent with applicable laws and regulations, provide for sanctions, and contain such other provisions as the Director of the FBI (acting for the Attorney General) may require. The security addendum, buttressed by ongoing audit programs of both the FBI and the sponsoring governmental agency, will provide an appropriate balance between the benefits of privatization, protection of individual privacy interests, and preservation of the security of the FBI's CHRI systems.

The FBI will develop a security addendum to be made available to interested governmental agencies. We anticipate that the security addendum will include physical and personnel security constraints historically required by NCIC security practices and other programmatic requirements, together with personal integrity and electronic security provisions comparable to those in NCIC User Agreements between the FBI and criminal justice agencies, and in existing Management Control Agreements between criminal justice agencies and noncriminal justice governmental entities. The security addendum will make clear that access to CHRI will be limited to those officers and employees of the private contractor or its subcontractor who require the information to properly perform services for the sponsoring governmental agency, and that the service provider may not access, modify, use, or disseminate such information for inconsistent or unauthorized purposes.

Consistent with such intent, Title 28 of the Code of Federal Regulations (C.F.R.) was amended to read:

§ 20.33 Dissemination of criminal history record information.

a) Criminal history record information contained in the Interstate Identification Index (III) System and the Fingerprint Identification Records System (FIRS) may be made available:

1) To criminal justice agencies for criminal justice purposes, which purposes include the screening of employees or applicants for employment hired by criminal justice agencies.

2) To noncriminal justice governmental agencies performing criminal justice dispatching functions or data processing/information services for criminal justice agencies; and

3) To private contractors pursuant to a specific agreement with an agency identified in paragraphs (a)(1) or (a)(6) of this section and for the purpose of providing services for the administration of criminal justice pursuant to that agreement. The agreement must incorporate a security addendum approved by the Attorney General of the United

> States, which shall specifically authorize access to criminal history record information, limit the use of the information to the purposes for which it is provided, ensure the security and confidentiality of the information consistent with these regulations, provide for sanctions, and contain such other provisions as the Attorney General may require. The power and authority of the Attorney General hereunder shall be exercised by the FBI Director (or the Director's designee).

This Security Addendum, appended to and incorporated by reference in a government-private sector contract entered into for such purpose, is intended to insure that the benefits of privatization are not attained with any accompanying degradation in the security of the national system of criminal records accessed by the contracting private party. This Security Addendum addresses both concerns for personal integrity and electronic security which have been addressed in previously executed user agreements and management control agreements.

A government agency may privatize functions traditionally performed by criminal justice agencies (or noncriminal justice agencies acting under a management control agreement), subject to the terms of this Security Addendum. If privatized, access by a private contractor's personnel to NCIC data and other CJIS information is restricted to only that necessary to perform the privatized tasks consistent with the government agency's function and the focus of the contract. If privatized the contractor may not access, modify, use or disseminate such data in any manner not expressly authorized by the government agency in consultation with the FBI.

FEDERAL BUREAU OF INVESTIGATION
CRIMINAL JUSTICE INFORMATION SERVICES
SECURITY ADDENDUM

The goal of this document is to augment the CJIS Security Policy to ensure adequate security is provided for criminal justice systems while (1) under the control or management of a private entity or (2) connectivity to FBI CJIS Systems has been provided to a private entity (contractor). Adequate security is defined in Office of Management and Budget Circular A-130 as "security commensurate with the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information."

The intent of this Security Addendum is to require that the Contractor maintain a security program consistent with federal and state laws, regulations, and standards (including the CJIS Security Policy in effect when the contract is executed), as well as with policies and standards established by the Criminal Justice Information Services (CJIS) Advisory Policy Board (APB).

This Security Addendum identifies the duties and responsibilities with respect to the installation and maintenance of adequate internal controls within the contractual relationship so that the security and integrity of the FBI's information resources are not compromised. The security program shall include consideration of personnel security, site security, system security, and data security, and technical security.

The provisions of this Security Addendum apply to all personnel, systems, networks and support facilities supporting and/or acting on behalf of the government agency.

1.00 Definitions

1.01 Contracting Government Agency (CGA) - the government agency, whether a Criminal Justice Agency or a Noncriminal Justice Agency, which enters into an agreement with a private contractor subject to this Security Addendum.

1.02 Contractor - a private business, organization or individual which has entered into an agreement for the administration of criminal justice with a Criminal Justice Agency or a Noncriminal Justice Agency.

2.00 Responsibilities of the Contracting Government Agency.

2.01 The CGA will ensure that each Contractor employee receives a copy of the Security Addendum and the CJIS Security Policy and executes an acknowledgment of such receipt and the contents of the Security Addendum. The signed acknowledgments shall remain in the possession of the CGA and available for audit purposes. The acknowledgement may be signed by hand or via digital signature (see glossary for definition of digital signature).

3.00 Responsibilities of the Contractor.

3.01 The Contractor will maintain a security program consistent with federal and state laws, regulations, and standards (including the CJIS Security Policy in effect when the contract is executed), as well as with policies and standards established by the Criminal Justice Information Services (CJIS) Advisory Policy Board (APB).

4.00 Security Violations.

4.01 The CGA must report security violations to the CJIS Systems Officer (CSO) and the Director, FBI, along with indications of actions taken by the CGA and Contractor.

4.02 Security violations can justify termination of the appended agreement.

4.03 Upon notification, the FBI reserves the right to:

a. Investigate or decline to investigate any report of unauthorized use;

b. Suspend or terminate access and services, including telecommunications links. The FBI will provide the CSO with timely written notice of the suspension. Access and services will be reinstated only after satisfactory assurances have been provided to the FBI by the CJA and Contractor. Upon termination, the Contractor's records containing CHRI must be deleted or returned to the CGA.

5.00 Audit

5.01 The FBI is authorized to perform a final audit of the Contractor's systems after termination of the Security Addendum.

6.00 Scope and Authority

6.01 This Security Addendum does not confer, grant, or authorize any rights, privileges, or obligations on any persons other than the Contractor, CGA, CJA (where applicable), CSA, and FBI.

6.02 The following documents are incorporated by reference and made part of this agreement: (1) the Security Addendum; (2) the NCIC 2000 Operating Manual; (3) the CJIS Security Policy; and (4) Title 28, Code of Federal Regulations, Part 20. The parties are also subject to applicable federal and state laws and regulations.

6.03 The terms set forth in this document do not constitute the sole understanding by and between the parties hereto; rather they augment the provisions of the CJIS Security Policy to provide a minimum basis for the security of the system and contained information and it is understood that there may be terms and conditions of the appended Agreement which impose more stringent requirements upon the Contractor.

6.04 This Security Addendum may only be modified by the FBI, and may not be modified by the parties to the appended Agreement without the consent of the FBI.

6.05 All notices and correspondence shall be forwarded by First Class mail to:

Assistant Director

Criminal Justice Information Services Division, FBI

1000 Custer Hollow Road

Clarksburg, West Virginia 26306

FEDERAL BUREAU OF INVESTIGATION

CRIMINAL JUSTICE INFORMATION SERVICES

SECURITY ADDENDUM

CERTIFICATION

I hereby certify that I am familiar with the contents of (1) the Security Addendum, including its legal authority and purpose; (2) the NCIC 2000 Operating Manual; (3) the CJIS Security Policy; and (4) Title 28, Code of Federal Regulations, Part 20, and agree to be bound by their provisions.

I recognize that criminal history record information and related data, by its very nature, is sensitive and has potential for great harm if misused. I acknowledge that access to criminal history record information and related data is therefore limited to the purpose(s) for which a government agency has entered into the contract incorporating this Security Addendum. I understand that misuse of the system by, among other things: accessing it without authorization; accessing it by exceeding authorization; accessing it for an improper purpose; using, disseminating or re-disseminating information received as a result of this contract for a purpose other than that envisioned by the contract, may subject me to administrative and criminal penalties. I understand that accessing the system for an appropriate purpose and then using, disseminating or re-disseminating the information received for another purpose other than execution of the contract also constitutes misuse. I further understand that the occurrence of misuse does not depend upon whether or not I receive additional compensation for such authorized activity. Such exposure for misuse includes, but is not limited to, suspension or loss of employment and prosecution for state and federal crimes.

_____ _____

Printed Name/Signature of Contractor Employee Date

_____ _____

Printed Name/Signature of Contractor Representative Date

_____

Organization and Title of Contractor Representative

APPENDIX I REFERENCES

White House Memo entitled "Designation and Sharing of Controlled Unclassified Information (CUI), May 9, 2008

[CJIS RA] *CJIS Security Policy Risk Assessment Report*; August 2008; For Official Use Only; Prepared by: Noblis; Prepared for: U.S. Department of Justice, Federal Bureau of Investigation, Criminal Justice Information Services Division, 1000 Custer Hollow Road, Clarksburg, WV 26306

[FBI SA 8/2006] *Federal Bureau of Investigation, Criminal Justice Information Services, Security Addendum*; 8/2006; Assistant Director, Criminal Justice Information Services, FBI, 1000 Custer Hollow Road, Clarksburg, West Virginia 26306

[FISMA] *Federal Information Security Management Act of* 2002; House of Representatives Bill 2458, Title III–Information Security

[FIPS 199] *Standards for Security Categorization of Federal Information and Information Systems*; Federal Information Processing Standards Publication, FIPS PUB 199; February 2004

[FIPS 200] *Minimum Security Requirements for Federal Information and Information Systems*; Federal Information Processing Standards Publication, FIPS PUB 200; March 2006

[FIPS 201] *Personal Identity Verification for Federal Employees and Contractors*; Federal Information Processing Standards Publication, FIPS PUB 201-1

[NIST SP 800–14] *Generally Accepted Principles and Practices for Securing Information Technology Systems*; NIST Special Publication 800–14

[NIST SP 800–25] *Federal Agency Use of Public Key Technology for Digital Signatures and Authentication*; NIST Special Publication 800–25

[NIST SP 800–30] *Risk Management Guide for Information Technology Systems*; NIST Special Publication 800–36

[NIST SP 800–32] *Introduction to Public Key Technology and the Federal PKI Infrastructure*; NIST Special Publication 800–32

[NIST SP 800–34] *Contingency Planning Guide for Information Technology Systems*; NIST Special Publication 800–34

[NIST SP 800–35] *Guide to Information Technology Security Services*; NIST Special Publication 800–35

[NIST SP 800–36] *Guide to Selecting Information Technology Security Products*; NIST Special Publication 800–36

[NIST SP 800–39] *Managing Risk from Information Systems, An Organizational Perspective*; NIST Special Publication 800–39

[NIST SP 800–40] *Procedures for Handling Security Patches*; NIST Special Publication 800–40

[NIST SP 800–44] Guidelines on Securing Public Web Servers; NIST Special Publication 800–44

[NIST SP 800–45] *Guidelines on Electronic Mail Security*; NIST Special Publication 800–45, Version 2

[NIST SP 800–46] *Security for Telecommuting and Broadband Communications*; NIST Special Publication 800–46

[NIST SP 800–48] *Wireless Network Security*: 802.11, *Bluetooth, and Handheld Devices*; NIST Special Publication 800–48

[NIST SP 800–52] *Guidelines on the Selection and Use of Transport Layer Security*; NIST Special Publication 800–52

[NIST SP 800–53] *Recommended Security Controls for Federal Information Systems*; NIST Special Publication 800–53, Revision 2

[NIST SP 800–53A] *Guide for Assessing the Security Controls in Federal Information Systems, Building Effective Security Assessment Plans*; NIST Special Publication 800–53A

[NIST SP 800–58] *Security Considerations for Voice over IP Systems*; NIST Special Publication 800–58

[NIST SP 800–60] *Guide for Mapping Types of Information and Information Systems to Security Categories*; NIST Special Publication 800–60, Revision 1, DRAFT

[NIST SP 800–63–1] *Electronic Authentication Guideline*; NIST Special Publication 800–63–1; DRAFT

[NIST SP 800–64] NIST Special Publication 800–64

[NIST SP 800–66] *An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act* (HIPAA); NIST Special Publication 800–66

[NIST SP 800–68] *Guidance for Securing Microsoft Windows XP Systems for IT Professionals: A NIST Security Configuration Checklist*; NIST Special Publication 800–68

[NIST SP 800–70] *Security Configuration Checklists Program for IT Products*; NIST Special Publication 800–70

[NIST SP 800–72] *Guidelines on PDA Forensics*; NIST Special Publication 800–72

[NIST SP 800–73] *Integrated Circuit Card for Personal Identification Verification*; NIST Special Publication 800–73; Revision 1

[NIST SP 800–76] *Biometric Data Specification for Personal Identity Verification*; NIST Special Publication 800–76

[NIST SP 800–77] *Guide to IPSec VPNs*; NIST Special Publication 800–77

[NIST SP 800–78] *Cryptographic Algorithms and Key Sizes for Personal Identity Verification*; NIST Special Publication 800–78

[NIST SP 800–81] *Secure Domain Name System* (DNS) *Deployment Guide*; NIST Special Publication 800–81

[NIST SP 800–84] *Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities*; NIST Special Publication 800–84

[NIST SP 800–86] *Guide to Integrating Forensic Techniques into Incident Response*; NIST Special Publication 800–86

[NIST SP 800–87] *Codes for the Identification of Federal and Federally Assisted Agencies*; NIST Special Publication 800–87

[NIST SP 800–96] *PIV Card / Reader Interoperability Guidelines*; NIST Special Publication 800–96

[NIST SP 800–97] *Guide to* IEEE 802.11i: *Robust Security Networks*; NIST Special Publication 800–97

[NIST SP 800-121] *Guide to Bluetooth Security*, NIST Special Publication 800-121

[NIST SP 800-124] *Guidelines on Cell Phone and PDA Security*, NIST Special Publication 800-124

[OMB A–130] *Management of Federal Information Resources*; Circular No. A–130; Revised; February 8, 1996

[OMB M–04–04] *E-Authentication Guidance for Federal Agencies*; OMB Memo 04–04; December 16, 2003

[OMB M–06–15] *Safeguarding Personally Identifiable Information*; OMB Memo 06–15; May 22, 2006

[OMB M–06–16] *Protection of Sensitive Agency Information*; OMB Memo 06–16; June 23, 2006

[OMB M–06–19] *Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments*; OMB Memo 06–19; July 12, 2006

[OMB M–07–16] *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*; OMB Meme 07–16; May 22, 2007

[Surviving Security] *Surviving Security: How to Integrate People, Process, and Technology*; Second Edition; 2004

[USC Title 5, Section 552] *Public information; agency rules, opinions, orders, records, and proceedings*; United States Code, Title 5 - Government Agency and Employees, Part I - The Agencies Generally, Chapter 5 - Administrative Procedure, Subchapter II - Administrative Procedure, Section 552. Public information; agency rules, opinions, orders, records, and proceedings

[USC Title 44, Section 3506] *Federal Information Policy*; 01/02/2006; United States Code, Title 44 - Public Printing and Documents; Chapter 35 - Coordination of Federal Information Policy; Subchapter I - Federal Information Policy, Section 3506

APPENDIX J NONCRIMINAL JUSTICE AGENCY SUPPLEMENTAL GUIDANCE

This supplemental guidance for noncriminal justice agencies (NCJA) is provided specifically for those whose only access to FBI CJIS data is authorized by legislative enactment or federal executive order to request civil fingerprint-based background checks for licensing, employment, or other noncriminal justice purposes, via their State Identification Bureau and/or Channeling agency. This guidance does not apply to criminal justice agencies covered under an active user agreement with the FBI CJIS Division for direct connectivity to the FBI CJIS Division via the FBI CJIS Wide Area Network. Examples of the target audience for this supplemental guidance include school boards, banks, medical boards, gaming commissions, alcohol and tobacco control boards, social services agencies, pharmacy boards, etc. The information below identifies the sections of the CJIS Security Policy most closely related to the NCJA's limited scope of interaction with CJI.

1. The following CJIS Security Policy sections comprise the minimum standard requirements in all situations:
    a. 3.2.9 – Local Agency Security Officer (LASO)
    b. 5.1.1.6 – Agency User Agreements
    c. 5.1.1.7 – Security and Management Control Outsourcing Standard*
    d. 5.1.3 – Secondary Dissemination
    e. 5.2.1.1 – Security Awareness Training
    f. 5.3 – Incident Response
    g. 5.4.6 – Audit Record Retention
    h. 5.8 – Media Protection
    i. 5.9.2 – Controlled Area
    j. 5.11 – Formal Audits **
    k. 5.12 – Personnel Security***

    * Note: Outsourcing Standard applies when contracting with channeling or outsourcing agency.

    **Note: States shall periodically conduct audits of NCJAs. The FBI CJIS Division shall triennially conduct audits of a sampling of NCJAs.

    *** Note: See the National Crime Prevention and Privacy Compact Council's Outsourcing Standard for Contractor background check requirements.

2. Agencies located within states having passed legislation authorizing or requiring civil fingerprint-based background checks for personnel with access to criminal history record information for the purposes of licensing or employment shall follow the guidance in section 5.12. Agencies located within states without this authorization or

requirement are exempted from the fingerprint-based background check requirement until such time as appropriate legislation has been written into law.

3. When receiving CJI via encrypted e-mail or downloading from a web-site and subsequently storing the information as an encrypted electronic image Authorized Recipients should, in addition to all of the aforementioned sections, focus on compliance with policy sections:
    a. 5.5.2.4 – Access Control – Encryption
    b. 5.6 – Identification and Authentication (web-site access)
    c. 5.10.1.2 – System and Communications Protection – Encryption

4. When receiving CJI via e-mail or retrieving CJI from a website and subsequently storing the CJI electronically, Authorized Recipients should, in addition to 1.a–1.k above, focus on compliance with policy sections:
    a. 5.5.2.4 – Access Control – Encryption
    b. 5.6 – Identification and Authentication
    c. 5.7 – Configuration Management
    d. 5.10 – System and Communications Protection and Information Integrity

5. If an NCJA further disseminates CJI via encrypted e-mail to Authorized Recipients, located outside the NCJA's designated controlled area, the NCJA should, in addition to 1.a–3.c above, focus on compliance with policy sections:
    a. 5.7 – Configuration Management
    b. 5.10 – System and Communications Protection and Information Integrity

6. If an NCJA further disseminates CJI via secure website posting to Authorized Recipients, located outside the NCJA's designated controlled area, the NCJA should focus on all sections outlined in 1.a-4.d above.

APPENDIX K CRIMINAL JUSTICE AGENCY SUPPLEMENTAL GUIDANCE

This supplemental guidance is directed toward those criminal justice agencies that have historically not been subject to audit under the CJIS Security Policy guidelines. The target audience typically gains access to CJI via fax, hardcopy distribution or voice calls; does not have the capability to query state or national databases for criminal justice information; and, may have been assigned an originating agency identifier (ORI) but is dependent on other agencies to run queries on their behalf. This guidance does not apply to criminal justice agencies covered under an active information exchange agreement with another agency for direct or indirect connectivity to the state CSA – in other words those agencies traditionally identified as "terminal agencies". The information below identifies the sections of the CJIS Security Policy the target audience will most often encounter:

1. The following CJIS Security Policy sections comprise the minimum standard requirements in all situations:
    a. 3.2.9 – Local Agency Security Officer (LASO)
    b. 5.1.1.3 – Criminal Justice Agency User Agreements
    c. 5.1.3 – Secondary Dissemination
    d. 5.2.1.1 – Security Awareness Training
    e. 5.3 – Incident Response
    f. 5.4.6 – Audit Record Retention
    g. 5.8 – Media Protection
    h. 5.9 – Physical Security
    i. 5.10.2 – Facsimile Transmission of CJI
    j. 5.11 – Formal Audits*
    k. 5.12 – Personnel Security

    *Note: States shall triennially audit all CJAs

2. When receiving CJI via encrypted e-mail or downloading from a web-site and subsequently storing the information as an encrypted electronic image Authorized Recipients should, in addition to all of the aforementioned sections, focus on complying with policy sections:
    a. 5.5.2.4 – Access Control – Encryption
    b. 5.6 – Identification and Authentication
    c. 5.10.1.2 – System and Communications Protection – Encryption

3. When receiving CJI via e-mail or retrieving CJI from a website and subsequently storing the CJI electronically, Authorized Recipients should, in addition to 1.a–1.k above, focus on complying with policy sections:
    a. 5.5.2.4 – Access Control – Encryption
    b. 5.6 – Identification and Authentication
    c. 5.7 – Configuration Management
    d. 5.10 – System and Communications Protection and Information Integrity

Exhibit 6

Regional Interlocal Agreement

Broward County
Office of Communications Technology

Regional Interlocal Agreement

Table of Contents

I. Agreement

II. Exhibit A – Statement of Work, System Description, and Acceptance Test Plan

III. Exhibit B – Demarcation Points

IV. Exhibit C – Equipment List

V. Exhibit D – Change Management Request Procedure

VI. Exhibit E – Project Charter

VII. Exhibit F – Service Level Agreement

VIII. Exhibit G – Trunked Radio System Standard Operating Procedures

IX. Exhibit H - Radio Subscriber Responsibilities

AGREEMENT

BETWEEN

BROWARD COUNTY

and

SHERIFF OF BROWARD COUNTY, FLORIDA

Providing for

COOPERATIVE PARTICIPATION IN A

REGIONAL PUBLIC SAFETY INTRANET

This is an Interlocal Agreement, made and entered into by and between Broward County (hereinafter referred to as "COUNTY"), a political subdivision of the State of Florida, and SHERIFF of Broward County, Florida, a political subdivision of the State of Florida, (hereinafter referred to as "SHERIFF"), collectively referred to as the "Parties," providing for cooperative participation in a Regional Public Safety Intranet ("RPSI").

WHEREAS, this Agreement is entered into pursuant to §163.01, Florida Statutes, also known as the "Florida Interlocal Cooperation Act of 1969;" and

WHEREAS, COUNTY is to establish, with cooperation of Broward cities, a county-wide interoperable public safety intranet that can support closest unit response in life-threatening emergencies and regional specialty teams; and

Whereas, the Parties desire to satisfy the intentions of the Broward County Charter by insuring that someone with a life-threatening emergency receive care from the closest available emergency vehicle; and

Whereas, the SHERIFF agrees to work towards insuring someone with a life-threatening emergency receive care from the closest available emergency vehicle. This includes pursuing automatic aid agreements with neighboring cities who utilize the county-wide CAD system; and

WHEREAS, the Parties desire to enhance radio interoperability by interconnecting COUNTY and SHERIFF public safety radio users; and

WHEREAS, the Parties desire to enhance information sharing by interconnecting COUNTY and SHERIFF public safety data users; and

WHEREAS, COUNTY maintains a Trunked Radio System as part of its public safety intranet that supports county-wide police, fire, and emergency services; and

WHEREAS, COUNTY maintains a Computer Aided Dispatching ("CAD") System as part of its public safety intranet that supports county-wide police, fire, and emergency services; and

WHEREAS, COUNTY maintains an Automated Vehicle Location ("AVL") System as part of its public safety intranet that supports county-wide police, fire, and emergency services; and

WHEREAS, COUNTY maintains a Law Records Management System ("LRMS") and a Fire Records Management System ("FRMS") as part of its public safety intranet that supports county-wide police, fire, and emergency services; and

WHEREAS, the Parties desire to make the most efficient use of their technical resources to enable the Parties to cooperate with each other to provide quality county-wide public safety communication services;

NOW, THEREFORE, IN CONSIDERATION of the mutual covenants and promises, set forth, the Parties agree as follows:

ARTICLE 1

DEFINITIONS

1.1	Advanced Tactical Mapping ("ATM"): A component of the RPSI that provides computer aided dispatch mapping. In conjunction with AVL, these maps pinpoint the real time location, availability, status, and routing of emergency vehicles which ultimately enhance response times.
1.2	Automated Vehicle Location ("AVL") System: A component of the RPSI that provides GPS-based tracking of public safety vehicles. AVL facilitates closest unit response when coupled with a common CAD platform.
1.3	Change Management Requests ("CMR"): The CMR process will be used to specify the times and conditions when designated tasks can be performed on all software and

	hardware affiliated with the RPSI including but not limited to the Trunked Radio System, Public Safety Network, Computer Aided Dispatch (CAD) System, E-911, etc. The CMR is more fully explained in Exhibit "D".
1.4	Computer Aided Dispatch ("CAD") System: A component of the RPSI that has as one of its functions, in conjunction with the AVL System, the ability to assist a radio dispatcher in identifying and dispatching public safety vehicles and personnel closest to the scene of an incident.
1.5	Contract Administrator: COUNTY's Contract Administrator of the Regional Public Safety Intranet "RPSI" is COUNTY's Director of the Office of Communications Technology.
1.6	Demarcation Points: A "Demarcation Point" or "Demarc" identifies a responsibility boundary between SHERIFF-responsible items and COUNTY-responsible items. EXHIBIT "B" further defines and visually portrays the RPSI Demarcation Points and entity-responsibilities on a portion by portion basis.
1.7	Equipment: The COUNTY-owned and maintained items listed in EXHIBIT "C" and any other COUNTY-provided items.
1.8	Fire Records Management System ("FRMS"): A component of the RPSI that archives fire-related dispatch records and information.
1.9	Fire Rescue Frontline Vehicles: Refers to those vehicles typically dispatched in the initial stages of an incident for the protection and preservation of life, property, and the environment. Vehicles whose primary purpose is responding to emergencies where time is critical i.e.; Fire Engines (Pumpers), Ladder Trucks, Medical Rescue Vehicles, and Shift Commanders. Frontline vehicles are staffed and dispatched and not in a reserve or staff capacity.
1.10	Fire Station Alerting: Allows regional and non-regional communication centers to efficiently respond to emergencies by managing the assets of multiple fire stations. Public Safety

	Dispatch Centers can dispatch an engine, ambulance, entire station, or multiple stations by selecting them on their PC screen or by the push of a few buttons.
1.11	Law Records Management System ("LRMS"): A component of the RPSI that archives law enforcement dispatch records and information.
1.12	NetMotion: A component of the RPSI that improves mobile data network performance, encryption, communication stability, and roaming between disparate private and public wireless networks.
1.13	Network Mobility Zone ("NMZ"): A component of the RPSI which extends the public safety network to multiple jurisdictions. The network mobility zone provides the mobile data and remote facility user's access to the core of the Public Safety Intranet applications.
1.14	Non-Dispatch Facility: A SHERIFF owned facility hosted by the infrastructure, applications, and services of the RPSI. A non-dispatch facility does not receive E-911 calls nor does it provide SHERIFF-wide or county-wide dispatch services. A non-dispatch facility may require access to FRMS, Read-Only CAD Services, and PMDC via their owned and operated Local Area Networks. The SHERIFF-COUNTY demarcation boundaries are outlined in "Exhibit B".
1.15	Peripheral Equipment: The SHERIFF-owned and maintained items listed in Exhibit "C" and any other SHERIFF-provided items. Peripheral equipment includes but is not limited to Ethernet cabling, mouse, keyboard, speakers, printers, etc.
1.16	Project: The integration of a regional public safety intranet comprised of radio and data systems, benefiting public safety agencies within Broward County that choose to participate.
1.17	Project Charter: Outlines the requirements, direction, constraints, and collectively accepted deliverables within a project. In addition, the charter will act as a guideline for the project manager and project team members to establish scope, schedule, and cost pertaining to the Project. The Project Charter template is further explained and listed in Exhibit "E".

1.18	Project Manager: An employee of the COUNTY who is assigned by the Contract Administrator to provide day-to-day management of the Project from inception to completion.
1.19	Public Safety Network ("PSN"): A component of the RPSI which provides the communication connectivity and network infrastructure for data portions of the RPSI.
1.20	Regional Dispatch Center (RDC): A cooperative dispatch center providing E911 call taking and dispatch services for multiple jurisdictions. A RDC is also hosted by the infrastructure, applications, and services of the RPSI. A RDC supports the overall goals of closest unit response, radio interoperability, and data sharing and is directly connected and utilizes the Regional CAD and County-Wide Radio System.
1.21	Regional Public Safety Intranet ("RPSI"): The overall collection of Equipment – including but not limited to COUNTY's Trunked Radio System – Public Safety Network – Public Safety Applications – that constitutes the Regional Public Safety Intranet. SHERIFF-owned equipment interfaces to the COUNTY-owned RPSI.
1.22	Service Level Agreements ("SLA"): Defines an expected level of service segregated into various categories: System performance, trouble resolution, operations, and administration. The Service Level Agreements are further explained and listed in Exhibit "F".
1.23	SmartZone: A component of the RPSI that interconnects disparate radio systems to provide county-wide coverage for roaming, efficient use of channels, and voice communication interoperability.
1.24	Subscriber Maintenance: Refers to SHERIFF's responsibility to maintain the SHERIFF owned user's equipment. Subscriber maintenance is further explained in Exhibit "B".
1.25	System Maintenance: Refers to COUNTY's responsibility to maintain the regional public safety intranet (RPSI) as described in Exhibit "B".

1.26	Trunked Radio System: COUNTY's Trunked Radio Communications System, a major portion of which is used by police and fire rescue personnel within Broward COUNTY's Office. Today, COUNTY owns and operates a twenty-eight (28) channel 800 MHz trunked simulcast SmartZone radio system.

ARTICLE 2

SCOPE OF WORK

2.1 COUNTY and SHERIFF agree to install the necessary Equipment and Peripheral Equipment and perform their respective required tasks in accordance with the Statement of Work (EXHIBIT "A").

2.2 The work to be done shall be referenced, for convenience, according to the project designations and as further identified and detailed in the EXHIBIT "A" Statement of Work.

2.3 COUNTY agrees that the Trunked Radio System will meet appropriate coverage, functionality, and availability parameters and accepted industry standard levels of performance as determined by Federal Communications Commission (FCC), Telecommunications Industries Association (TIA), and Association of Public Safety Communication Officials (APCO) standards together with manufacturers' specifications.

2.4 COUNTY shall own all Equipment the COUNTY supplies to SHERIFF pursuant to this agreement.

2.5 SHERIFF shall provide COUNTY access to the SHERIFF's equipment rooms to the extent required for the installation of the COUNTY's owned equipment and integration of any applicable SHERIFF system into the RPSI. SHERIFF will exercise due care to ensure that the electrical, security, and environmental requirements are maintained for such equipment rooms.

2.6 COUNTY agrees that the CAD, AVL, FRMS, LRMS, Mobility Zone, and Public Safety Network functionalities supplied to SHERIFF shall also meet appropriate performance levels as defined in EXHIBIT "A".

2.7 The Regional Public Safety Intranet will perform based on the specifications of any given application being run on the system as defined in the EXHIBIT "A" Statement of Work. The RPSI shall allow for exchange of information amongst public safety users.

2.8 SHERIFF shall be responsible for supplying COUNTY with needed uninterruptible power system (UPS) electrical power, electrical wiring, heating ventilating and air conditioning (HVAC), and standby power generation – to meet manufacturer guidelines and operational standards established by COUNTY for dispatch center Equipment.

2.09 SHERIFF agrees to comply with the Demarcation Point division of responsibilities for the RPSI as provided in EXHIBIT "B".

2.10 COUNTY shall maintain all systems outlined as "COUNTY responsibility" in EXHIBIT "B" over the life of this Agreement.

2.11 SHERIFF shall maintain all systems outlined as "SHERIFF responsibility" in EXHIBIT "B" over the life of this Agreement.

2.12 COUNTY shall not be responsible for the payment of any taxes, insurance, and utilities for SHERIFF owned facilities.

2.13 Access to SHERIFF's facilities for COUNTY personnel, or COUNTY's subcontractors, consistent with SHERIFF security practices and procedures, shall be unlimited as to time and day.

2.14 SHERIFF shall be responsible for any and all maintenance and repairs to the existing SHERIFF owned facilities and any upgrades to such facilities. SHERIFF shall maintain the structural and operational integrity of all associated SHERIFF owned facilities and supporting equipment including but not limited to: batteries, buildings, cable plant, generators, roof, skylights, walls, foundations, sidewalks, floors, windows, ceilings, sprinkler and hot water systems, elevators, heating systems, air conditioning systems, plumbing, electrical and all other structural components.

2.15 Prior to the issuance of the Notice to Proceed from the COUNTY's Contract Administrator to the Contractor, the Parties shall develop a mutually acceptable Project Plan inclusive of project charter ("Exhibit E"), project schedule, and communication plan set forth, among other things, (i) selected tasks, deliverables, and activities required of each party, including all dates by which the responsible party must complete such activity, (ii) the milestones and the agreed upon date for completion of each milestone; and (iii) the date for System Acceptance. This development shall constitute a Detailed Design Review. The Project Schedule shall be in the form of a progress chart of suitable scale to appropriately indicate the percentage of work scheduled for completion at any time. Each party represents that it will act in good faith to establish the Project Schedule within thirty (30) days of a signed contract between

the COUNTY's Contract Administrator and the Contractor and that the number of days established will be reasonable as to each activity.

2.16 Upon SHERIFF's concurrence with, and COUNTY's acceptance of, the Detailed Design Review and Project Schedule submitted to COUNTY, COUNTY will provide contractor with a Notice to Proceed.

2.17 Effective with the execution of this Agreement, SHERIFF shall become a voting member of the Regional Public Safety Communications Committee ("RPSCC") or equivalent committee that has the authority to make technical decisions with regard to major upgrades and configuration changes to the RPSI.

2.18 SHERIFF shall follow all RPSI Trunked Radio System policies and standard operating procedures in place at the time of this Agreement, a list of which are included in Exhibit "G" as well as those developed in the future and issued to SHERIFF by COUNTY. SHERIFF agrees to comply with any enforcement actions required by these policies and procedures for mis-use or abuse of the RPSI Trunked Radio System.

2.19 COUNTY and SHERIFF shall jointly be responsible for developing desired fleet mapping and programming of all subscriber units and system parameters necessary to meet the operational requirements as provided in Exhibit H.

2.20 SmartZone operation shall be limited to public safety users only.

2.21 SHERIFF acknowledges that the services to be performed under this Agreement, relative to COUNTY's responsibilities, shall be performed by COUNTY and/or its contractors and shall be under the sole supervision and direction of COUNTY. At SHERIFF facilities, SHERIFF may monitor installation work done by the COUNTY, its employees, agents, and subcontractors. Likewise, COUNTY acknowledges that the services to be performed under this Agreement relative to SHERIFF's responsibilities shall be performed by SHERIFF and/or its contractor(s) and shall be under the sole supervision and direction of SHERIFF. COUNTY may monitor installation work done by the SHERIFF, its employees, agents, and subcontractors.

2.22 SHERIFF is responsible for Subscriber Maintenance including repair and sub-fleet additions, moves, and changes to SHERIFF subscribers as provided in Exhibit "H". SHERIFF may utilize the services of a third party to provide maintenance of SHERIFF subscribers, or SHERIFF may contract with COUNTY for a fee for a combination of the aforementioned services or for all of the above services as provided in Exhibit H.

2.23 SHERIFF is responsible for all removals and installations of its subscriber equipment.

2.24 COUNTY agrees that it will not implement any changes/enhancements to the RPSI that could adversely affect the SHERIFF system subscribers unless directed to do so by Federal or State mandates as stated in Section 3.3 of this Agreement or otherwise agreed to, in writing, between the Parties. Prior written notice as defined in Exhibit "D" shall be made by COUNTY to SHERIFF for proposed changes and their potential effect on SHERIFF operations. Should SHERIFF or COUNTY desire to perform changes to the facility or the RPSI that may impact the Equipment or services provided by the COUNTY, the Change Management Request (CMR) procedures (Exhibit "D") will be followed.

2.25 The parties agree that any and all drawings, plans, specifications or other documents or materials will be reviewed by SHERIFF and COUNTY, or its sub-contractors to ensure that they are: (a) consistent with the SHERIFF and COUNTY requirements for the Project; (b) sufficiently fit and proper for the purposes intended; and (c) comply with all applicable laws, statutes, building codes, and SHERIFF and COUNTY guidelines or regulations, which apply to or govern the Project. SHERIFF's approval, acceptance, use of or payment for all or any part of COUNTY's services under this Agreement or of the Project itself shall in no way alter COUNTY's obligations or SHERIFF's rights. Copies of all items shall be provided to SHERIFF and COUNTY. The Project Charter listed as Exhibit "E" will be used to identify the requirements and expectations set forth by SHERIFF and COUNTY.

2.26 In the event that COUNTY or SHERIFF believe that any aspect of a Project is not in compliance with approved plans or applicable codes, or that work cannot be completed as designated, COUNTY or SHERIFF shall notify the appropriate other party within the next business day after discovery, in writing or electronically, as to the reason(s) the proposed portion of the work is not in compliance or not feasible to meet the scope of services to be provided in this Agreement.

2.27 SHERIFF agrees to complete a joint Acceptance Test Plan (EXHIBIT "A" Attachment 2) with COUNTY to inspect COUNTY's or the Contractor's performed work on the System to determine if it meets the SHERIFF's operational needs and COUNTY's requirements.

2.28 SHERIFF public safety users shall have equal accessibility to COUNTY's RPSI similar to other criminal justice agency and fire subscribers.

2.29 SHERIFF agrees to purchase all necessary SHERIFF subscriber

equipment as described in Exhibit "B" within ninety (90) days of the SHERIFF providing written notice to COUNTY exercising its option to participate in a regional public safety intranet consisting of any one or combination of the following: Trunked Radio System, CAD, ATM, AVL, FRMS, LRMS, or PSN.

2.30 SHERIFF agrees to provide COUNTY or COUNTY's Contractor, for the term of the Agreement, with facility space associated with the on-site maintenance, troubleshooting, and repair of all COUNTY Equipment.

ARTICLE 3

TERM

3.1 The obligation of the Parties to perform under this Agreement shall commence upon the date of the last party executing this Agreement.

3.2 The term of this Agreement shall be for five (5) years from the commencement date pursuant to Section 3.1 above. This Agreement may be renewed every five (5) years with the approval of both COUNTY and SHERIFF, unless terminated pursuant to Article 4.

3.3 The terms of this Agreement may be amended if a state or federal regulatory agency mandates significant technological modifications of the system requiring a major reconfiguration or upgrade. In such instances, the Parties shall meet to determine an appropriate solution and funding. In the event the parties are unable to reach an agreement regarding state or federal mandates for technological modifications and/or funding of said modifications, either party may terminate the Agreement for cause pursuant to Article 4.

ARTICLE 4

TERMINATION

4.1 This Agreement may not be terminated by the COUNTY or SHERIFF for convenience during the initial five (5) year term with the exception of the circumstances set forth in Paragraph 4.3. Any subsequent renewal term may be terminated for either cause or convenience by either party upon providing written notice to the other party at least two (2) years prior to the effective date of such termination.

4.2 The failure of the either party to perform its responsibilities as set forth herein for a period of thirty (30) calendar days after written notice by the non-breaching party shall constitute a breach of this Agreement. In the

event the party in breach fails to cure the breach within such thirty (30) day period, the other party may immediately terminate this Agreement upon written notice to the party in breach of the Agreement.

4.3 SHERIFF recognizes that the Board of County Commissioners, Broward County, Florida is the authority which establishes, allocates or otherwise provides for COUNTY's budget year funding. If in any budget year, funding, for any reason, is not provided to cover the COUNTY's responsibilities and obligations under this Agreement, this Agreement may be terminated by COUNTY without penalty upon written notice to the SHERIFF.

ARTICLE 5

COMPENSATION

5.1 Section 318.21(9), Florida Statutes, requires that Twelve dollars and fifty cents ($12.50) from each moving traffic violation must be used by the COUNTY to fund the COUNTY'S participation in an intergovernmental radio communication program approved by the Department of Management Services. SHERIFF understands such revenue generated within its jurisdiction will be used by the COUNTY to help fund the RPSI's operating costs.

ARTICLE 6

ADDITIONAL SERVICES

6.1 It is mutually acknowledged that during the term of this Agreement it may be desirable to change the scope or extent of the maintenance services or to have COUNTY substitute items of Equipment and/or provide new items of Equipment. The parties also recognize that during the term of this Agreement; additions, changes, or modifications may be necessary or desirable to carry out the intent or purpose of this Agreement. The Parties agree that during the term of this Agreement they will negotiate in good faith any requested changes to the scope or extent of the maintenance services or to substitution of items of Equipment and/or provision of new items of Equipment and other services proposed by COUNTY. All requested changes to the scope or extent of the maintenance services or to substitution of items of Equipment and/or provision of new items of Equipment, upgrades and other proposed additional services are subject to funding availability.

6.2 Any and all modifications to the terms and conditions of this Agreement must be contained in a written amendment executed with the same formalities as set forth herein. Should SHERIFF or COUNTY desire to

perform changes to the facilities, the RPSI or PSN that may adversely impact the Equipment provided by the COUNTY, the Change Management Request (CMR) procedures (Exhibit "D") will be followed.

ARTICLE 7

LIABILITY

7.1 SHERIFF and COUNTY shall each individually defend any action or proceeding brought against their respective agency pursuant to this Agreement and shall be individually responsible for all of their respective costs, attorneys' fees, expenses and liabilities incurred as a result of any such claims, demands, suits, actions, damages and causes of action, including the investigation or their defense thereof, and from and against any orders, judgments or decrees which may be entered as a result thereof.

7.2 SHERIFF and COUNTY agree that no indemnification or hold harmless agreement shall be in effect concerning any claims, demands, damages and causes of action which may be brought against either party pursuant to this Agreement.

7.3 SHERIFF and COUNTY are state agencies or political subdivisions as defined in Section 768.28, Florida Statutes, and agree to be fully responsible for acts and omissions of its agents or employees to the extent required by law. Noting herein is intended to serve as a waiver of sovereign immunity by any party to which sovereign immunity is applicable. Nothing herein shall be construed as consent by a state agency or political subdivision of the State of Florida to be sued by third parties in any matter, whether arising out of this Agreement or any other contract.

ARTICLE 8

INSURANCE

8.1 The Parties acknowledge that COUNTY is self insured in accordance with the provisions set forth in Section 768.28, Florida Statutes.

ARTICLE 9

PERFORMANCE

9.1 Operational Performance Metrics will be provided by COUNTY to SHERIFF on a quarterly basis to collectively evaluate system integrity. The operational performance metrics will be a part of the service level agreement provided by COUNTY to SHERIFF and further explained in "Exhibit F".

ARTICLE 10

CONFIDENTIALITY

10.1 COUNTY, to the extent permitted by law, shall not disclose confidential Information provided by or obtained from SHERIFF in connection with the services performed under this Agreement. Confidential Information shall mean criminal intelligence information, criminal investigative information, computer programs and application software, embedded software and their documentation. SHERIFF shall expressly identify in writing the confidential information.

10.2 If either party is confronted with legal action or believes applicable law requires it to disclose any portion of the other party's Confidential Information hereunder, that party shall promptly notify and assist the other (at the other party's expense) in obtaining a protective order or other similar order, and shall thereafter disclose only the minimum of the other party's Confidential Information that is required to be disclosed in order to comply with the legal action, whether or not a protective order or other order has been obtained.

10.3 COUNTY acknowledges that a breach of this provision will cause irreparable injury to SHERIFF, that the remedy at law for any such violation or threatened violation will not be adequate and that SHERIFF shall be entitled to seek temporary and permanent injunctive relief.

10.4 The provisions of this Section shall remain in full force and effect and enforceable even after the expiration of this Agreement.

ARTICLE 11

RECORDS

COUNTY shall keep such records and accounts as may be necessary in order to record complete and correct entries for charges and any expenses for which COUNTY expects to be paid. All books and records relative to services under this Agreement will be available at all reasonable times for examination and audit by SHERIFF and shall be kept for a period of three (3) years after the completion of all

work to be performed pursuant to this Agreement. All books and records which are considered public records, pursuant to Chapter 119, Florida Statutes, shall be kept by COUNTY in accordance with such statutes.

ARTICLE 12

MISCELLANEOUS PROVISIONS

12.1 ASSIGNMENT: COUNTY shall perform the services provided for in this Agreement utilizing COUNTY's employees, contractors, and subcontractors. Said services shall be performed exclusively and solely for SHERIFF which is a Party to this Agreement. SHERIFF and COUNTY shall not have the right to assign this Agreement without the express written approval of both parties.

12.2 JOINT PREPARATION: The Parties acknowledge that they have sought and received whatever competent advice and counsel as was necessary for them to form a full and complete understanding of all rights and obligations herein and that the preparation of this Agreement has been their joint effort. The language agreed to expresses their mutual intent and the resulting document shall not, solely as a matter of judicial construction, be construed more severely against one of the Parties than the other.

12.3 SEVERABILITY: The invalidity of any provision of the Agreement shall in no way affect the validity of any other provision.

12.4 ENTIRE AGREEMENT AND MODIFICATION: This Agreement incorporates, supersedes and includes all prior negotiations, correspondence, conversations, agreements or understandings applicable to the matter contained herein. It is further agreed that no change, alteration or modification in the terms and conditions contained herein shall be effective unless contained in a written document executed with the same formality and of equal dignity herewith.

12.5 COMPLIANCE WITH LAWS: Each Party shall comply with all federal, state, and local laws, codes, ordinances, rules and regulations in performing its duties, responsibilities and obligations pursuant to this Agreement.

12.6 BINDING EFFECT: This Agreement shall be binding upon and inure to the benefit of the Parties hereto and their respective successors.

12.7 FORCE MAJEURE: Neither party shall be obligated to perform any duty, requirement or obligation under this Agreement if such performance is prevented by fire, hurricane, earthquake, explosion, wars, sabotage,

accident, flood, acts of God, strikes, or other labor disputes, riot or civil commotions, or by reason of any other matter or conditions beyond the control of either party, and which cannot be overcome by reasonable diligence and without unusual expense ("Force Majeure").

12.8 AUTHORITY: The individuals executing this Agreement on behalf of any entity do hereby represent and warrant that they are, on the date of this Agreement, duly authorized by all necessary and appropriate action to execute this Agreement on behalf of their principal.

12.9 NOTICES: With the exception of provisions of Paragraph 2.28, all notices given or required under this Agreement shall be in writing and may be delivered in person or by United States mail, postage prepaid, first class and certified, return receipt requested, addressed as follows:

COUNTY:

Broward County
Director – Office of Communications Technology
115 S. Andrews Avenue, Room 325
Fort Lauderdale, FL 33301

With a copy to: County Attorney
Office of the County Attorney
115 S. Andrews Avenue, Room 423
Fort Lauderdale, FL 33301

SHERIFF:

Broward Sheriff's Office
Director – Office of Information Technology
2601 W Broward Blvd
Fort Lauderdale, FL 33312

With a copy to: Ronald M. Gunzburger, General Counsel
Broward Sheriff's Office
2601 W Broward Blvd
Ft. Lauderdale, FL 33312

12.10 MATERIALITY AND WAIVER OF BREACH: The Parties agree that each requirement, duty, and obligation set forth herein is substantial and important to the formation of this Agreement and, therefore, is a material term hereof. Either Party's failure to enforce any provision of this

Agreement shall not be deemed a waiver of such provision or modification of this Agreement. A waiver of any breach of a provision of this Agreement shall not be deemed a waiver of any subsequent breach and shall not be construed to be a modification of the terms of this Agreement.

12.11 INDEPENDENT CONTRACTORS: The Parties agree that each party to this Agreement is an independent contractor. In providing such services, neither of the Parties, nor their respective agents shall act as officers, employees, or agents of the other party. This Agreement shall not constitute or make the Parties a partnership or joint venture.

12.12 RECORDING: This Agreement shall be recorded in accordance with the Florida Interlocal Cooperation Act of 1969.

12.13 PRIORITY OF PROVISIONS: If there is a conflict or inconsistency between any term, statement, requirement, or provision of any exhibit attached hereto, any document incorporated into this Agreement by reference and a term, statement, requirement, or provision of this Agreement, the term, statement, requirement, or provision contained in Articles 1 through 11 of this Agreement shall prevail and be given effect.

12.14 MULTIPLE ORIGINALS: This Agreement may be fully executed in five (5) copies by all Parties, each of which, bearing original signatures, shall be the force and effect of an original document.

12.15 NON-DISCRIMINATION: The Parties shall not discriminate against any employee or participant in the performance of the duties, responsibilities and obligations under this Agreement because of race, age, religion, color, gender, disability, marital status, sexual orientation or national origin.

12.16 RECORDS: Each party shall maintain its own respective records and documents associated with this Agreement in accordance with the records retention requirements applicable to public records. Each party shall be responsible for compliance with any public documents requests served upon it pursuant to Section 119.07, Florida Statutes, and any resultant award of attorney's fees for noncompliance with that law.

12.17 DRAFTING: This Agreement has been negotiated and drafted by all Parties hereto and shall not be more strictly construed against any party because of such party's preparation of this Agreement.

12.18 CHOICE OF LAW, WAIVER OF JURY TRIAL: Any controversies or legal problems arising out of this transaction and any action involving the enforcement or interpretation of any rights hereunder shall be submitted to the jurisdiction of the State courts of the Seventeenth Judicial Circuit of Broward County, Florida, or the United States District Court, Southern

District, Broward County, Florida, the venue sites, and shall be governed by the laws of the state of Florida and any applicable federal laws, codes or regulations. To encourage prompt and equitable resolution of any litigation that may arise hereunder, each party hereby waives any rights it may have to a trial by jury in any such litigation.

12.19 OWNERSHIP OF EQUIPMENT: COUNTY retains ownership of all Equipment that the COUNTY provides to the SHERIFF pursuant to the terms and conditions of this Agreement. In the event this Agreement is terminated by either party, the COUNTY shall remove and/or recover all equipment within ninety (90) days of the effective date of termination.

12.20 ATTACHMENTS AND REFERENCES: The following named exhibits are made an integral part of this Agreement:

EXHIBIT "A": Statement of Work
- Attachment 1: System Description
- Attachment 2: Acceptance Test Plan

EXHIBIT "B": System Demarcation Points
- Attachment 1A: Regional Dispatch Center
- Attachment 1B: Non-Dispatch Facility
- Attachment 1C: Mobile Data Law Enforcement
- Attachment 1D: Mobile Data Fire Rescue
- Attachment 2: Demarcation Drawings

EXHIBIT "C": Equipment List

EXHIBIT "D": Change Management Request

EXHIBIT "E": Project Charter

EXHIBIT "F": Service Level Agreements
- Attachment 1: Terms and Conditions
- Attachment 2: Trouble Ticket Workflow

EXHIBIT "G": RPSI Trunked Radio System SOP's

12.21 THIRD PARTY BENEFICIARIES: This Agreement is not intended to benefit any third party nor shall it create a contractual relationship with any third party.

THE REMAINDER OF THIS PAGE IS INTENTIONALLY LEFT BLANK

IN WITNESS WHEREOF, the parties hereto have made and executed this Agreement: BROWARD COUNTY through its BOARD OF COUNTY COMMISSIONERS, signing by and through its Mayor or Vice-Mayor, authorized to execute same by Board action on the _____ day of _____, 20__, and SHERIFF, signing by and through its _____, duly authorized to execute same.

COUNTY:

ATTEST:

BROWARD COUNTY, by and through its Board of County Commissioners

_____
Broward County Administrator, as
Ex-officio Clerk of the Broward County
Board of County Commissioners

By_____
Mayor

_____ day of _____, 20___

Approved as to form by
Office of the County Attorney
for Broward County, Florida
JONI ARMSTRONG COFFEY, County Attorney

Governmental Center, Suite 423
115 South Andrews Avenue
Fort Lauderdale, Florida 33301
Telephone: (954) 357-7600
Telecopier: (954) 357-6968

Insurance requirements
approved by Broward County
Risk Management Division

By _____ 2/20/13
(Date)
Risk Management Division
Jacqueline A. Binns
Risk Insurance and
Contracts Manager

By_____
Noel M. Pfeffer, Deputy County Attorney

INTERLOCAL AGREEMENT BETWEEN BROWARD COUNTY AND THE SHERIFF OF BROWAD COUNTY FOR COOPERATIVE PARTICIPATION IN A REGIONAL PUBLIC SAFETY INTRANET.

SHERIFF OF BROWARD COUNTY

By: _____ Date: 2/19/13
SCOTT J. ISRAEL,
As Sheriff of Broward County

Approved as to form and legal sufficiency
subject to execution by the parties:

By: _____ Date: 021913
Ronald M. Gunzburger, General Counsel

EXHIBIT "B" – ATTACHMENT 1A

Regional Public Safety Intranet Demarcation Points

Regional Dispatch Center

RPSI Portion	Demarc	COUNTY Responsibility	CITY/SHERIFF Responsibility
Trunked Radio System	Gold Elite Console(s)	Infrastructure and software up to and including the COUNTY-owned Gold Elite/P25 IP based Radio Console(s) located in the Regional Dispatch Center.	All mobile and portable radio subscriber units including any software required to operate on the RPSI Trunked Radio System; and any advanced features and other monitoring equipment, as desired.
CAD System	CITY/SHERIFF LAN	Infrastructure and software up to and including the CAD server, Regional dispatch console workstations, Regional Dispatch CAD client licenses, and the needed communications via the RPSI.	All extended CITY/SHERIFF LAN equipment along with software, client licenses, peripheral equipment to provide communications to CITY/SHERIFF "read only" CAD workstations and all existing interfaces. (Future interfaces to the COUNTY-supplied systems do not apply.)
AVL System	CITY/SHERIFF LAN	Infrastructure up to and including the AVL server, regional client desktop software licenses, and the needed communications via the RPSI.	All extended CITY/SHERIFF LAN equipment along with software, client licenses, peripheral equipment to provide communications to SHERIFF "read only" CAD workstations and all existing interfaces. (Future interfaces to the COUNTY-supplied systems do not apply.)

RPSI Portion	Demarc	COUNTY Responsibility	CITY/SHERIFF Responsibility
Advanced Tactical Mapping	CITY/SHERIFF LAN	Infrastructure up to and including the advanced tactical mapping servers, regional standard desktop client software licenses, and the needed communications via the RPSI.	All extended CITY/SHERIFF LAN equipment along with software, client licenses, peripheral equipment to provide communications to CITY/SHERIFF “read only” CAD workstations and all existing interfaces. (Future interfaces to the COUNTY-supplied systems do not apply.)
Fire Records Management System	CITY/SHERIFF LAN	Infrastructure up to and including the Fire Records Management servers and standard software site and client licensing for Fire Records.	Desktop hardware and all LANs connected to the FRMS; non-standard or customized software desired by CITY/SHERIFF
Law Records Management System	CITY/SHERIFF LAN	Infrastructure up to and including the Law Records Management servers.	Desktop hardware and all LANs connected to the LRMS; non-standard or customized software desired by CITY/SHERIFF and standard software site and client licensing for Law Records.

EXHIBIT "B" – ATTACHMENT 1B

Regional Public Safety Intranet Demarcation Points

Non-Dispatch Facility

RPSI Portion	Demarc	COUNTY Responsibility	SHERIFF Responsibility
CAD System	CITY/SHERIFF LAN	Infrastructure up to and including physical network connectivity from the RPSI to a single pre-defined CITY/SHERIFF location.	All extended CITY/SHERIFF LAN equipment along with software, client licenses, desktop workstations, peripheral equipment to provide communications to CITY/SHERIFF "read only" CAD workstations and all existing interfaces. (Future interfaces to the COUNTY-supplied systems do not apply.)
Advanced Tactical Mapping	CITY/SHERIFF LAN	Infrastructure up to and including physical network connectivity from the RPSI to a single pre-defined CITY/SHERIFF location.	All extended CITY/SHERIFF LAN equipment along with software, client licenses, desktop workstations, peripheral equipment to provide communications to CITY/SHERIFF ATM workstations and all existing interfaces. (Future interfaces to the COUNTY-supplied systems do not apply.)
Fire Records Management System	CITY/SHERIFF LAN	Infrastructure up to and including physical network connectivity from the RPSI to a single pre-defined CITY/SHERIFF location. FRMS standard site and client desktop software licenses will be provided from COUNTY to CITY/SHERIFF.	Desktop hardware and all LANs connected to the FRMS; non-standard or customized software desired by CITY/SHERIFF
Law Records Management System	CITY/SHERIFF LAN	Infrastructure up to and including physical network connectivity from the RPSI to a single pre-defined CITY/SHERIFF location.	Desktop hardware and all LANs connected to the LRMS; non-standard or customized software desired by CITY/SHERIFF and standard software site and client licensing for Law Records.

EXHIBIT "B" – ATTACHMENT 1C

Regional Public Safety Intranet Demarcation Points

Mobile Data – Law Enforcement

RPSI Portion	Demarc	COUNTY Responsibility	CITY/SHERIFF Responsibility
Trunked Radio System	Gold Elite Console(s)	Infrastructure up to the COUNTY-owned Gold Elite/P25 IP Console(s) located in the Regional and/or Non-Regional Dispatch Center.	All mobile and portable radio subscriber units including any software required to operate on the RPSI Trunked Radio System; and any advanced features and other monitoring equipment, as desired.
CAD System	CITY/SHERIFF MDT	Infrastructure up to and including the CAD server and the needed communications via the RPSI.	All extended LAN equipment along with software, client licenses, peripheral equipment to provide communications to CITY/SHERIFF CAD MDT's and all existing interfaces. (Future interfaces to the COUNTY-supplied systems do not apply.)
AVL System	COUNTY's Server	Infrastructure up to and including the AVL server; and the needed communications via the RPSI.	All vehicle-related equipment and any remote monitoring equipment and software
Law Record Management System	COUNTY infrastructure	Infrastructure up to and including the Law Records Management servers.	All vehicle Equipment including laptop, modem, cabling, associated mounting hardware, antenna – and any monitoring Equipment and standard software site and client licensing for Law Records. Non-standard or customized software is also the responsibility of the CITY/SHERIFF.

EXHIBIT "B" – ATTACHMENT 1D

Regional Public Safety Intranet Demarcation Points

Mobile Data - Fire Rescue Frontline Vehicles

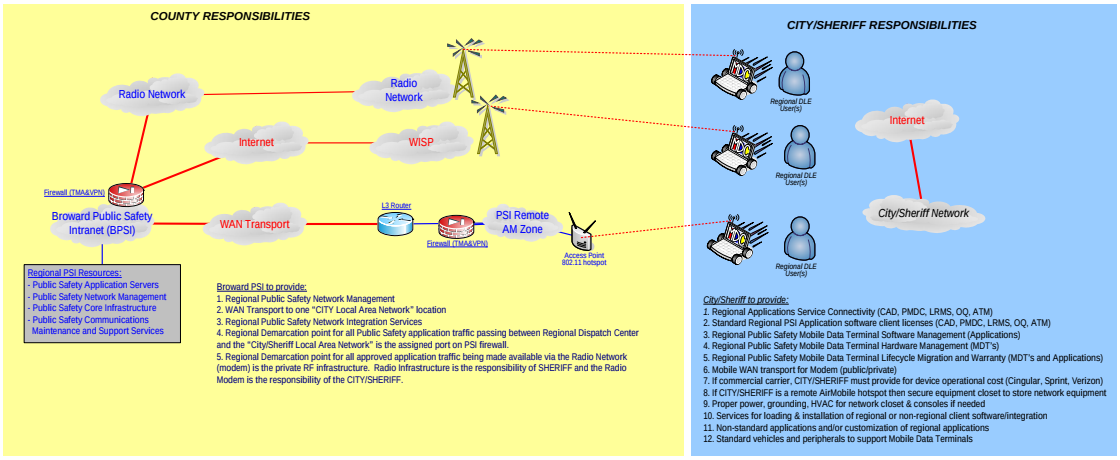
RPSI Portion	Demarc	COUNTY Responsibility	CITY/SHERIFF Responsibility
Trunked Radio System	Gold Elite Console(s)	Infrastructure up to the COUNTY-owned Gold Elite/P25 IP Console(s) located in the Regional and/or Non-Regional Dispatch Center.	All mobile and portable radio subscriber units including any software required to operate on the RPSI Trunked Radio System; and any advanced features and other monitoring equipment, as desired.
CAD System	CITY/SHERIFF LAN	Infrastructure and software up to and including the CAD server, MDT hardware, MDT regional CAD client software licenses, and the needed communications via the RPSI.	All vehicle related peripheral equipment and any monitoring equipment. Non-Regional or customized software desired by CITY/SHERIFF. (Future interfaces to the COUNTY-supplied systems do not apply.)
AVL System	Frontline Vehicle	Infrastructure up to and including the AVL server, and GPS devices located in Fire Rescue frontline vehicles.	All vehicle-related peripheral equipment and any remote monitoring equipment and software.

RPSI Portion	Demarc	COUNTY Responsibility	CITY/SHERIFF Responsibility
Mobile Data Terminals	Frontline Vehicle	COUNTY will assume capital and lifecycle procurement of MDT's and associated regional standard software for Fire Rescue frontline vehicles.	All vehicle related peripheral equipment and any monitoring Equipment. CITY/SHERIFF responsible for wireless modems and recurring operating costs. Non-regional or customized software desired by CITY/SHERIFF.
Fire Record Management System	COUNTY infrastructure	COUNTY infrastructure up to and including the FRMS Server and the needed communication interfaces via the RPSI.	Acquisition of FRMS standard site and client mobile software licenses will be the responsibility of CITY/SHERIFF. All vehicle related peripheral equipment and any monitoring Equipment. Non-regional or customized software desired by CITY/SHERIFF. (Future interfaces to the COUNTY-supplied systems do not apply.)

Broward County RPSI: ILA Mobile Data Law Enforcement

Broward County - Public Safety Intranet

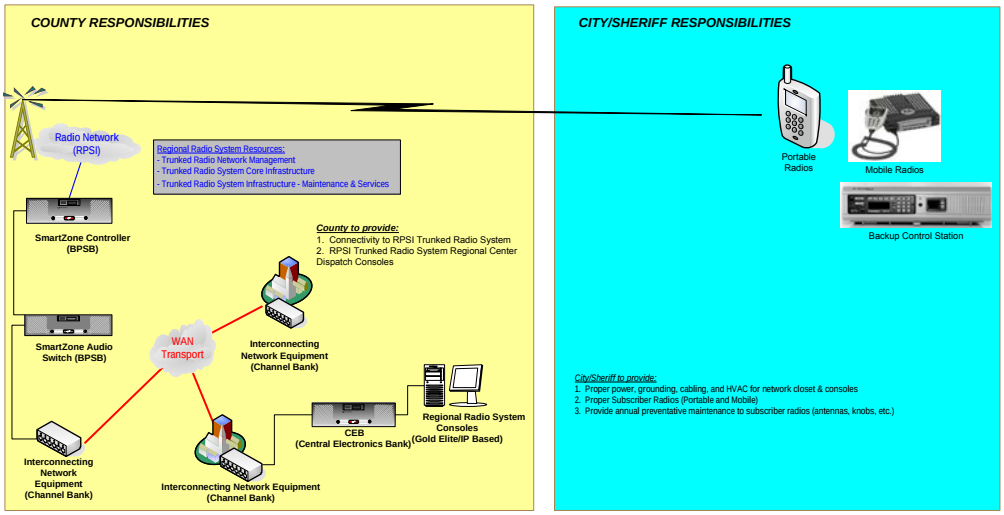
Logical Network Design Overview Mobile Data- Law Enforcement
Broward County/Sheriff/City Responsibilities



COUNTY – PSI – ILA: Mobile Data – Department of Law Enforcement | Sheet 4 of 7

Broward County-Radio Network: ILA Radio Demarc – Direct Subscribers

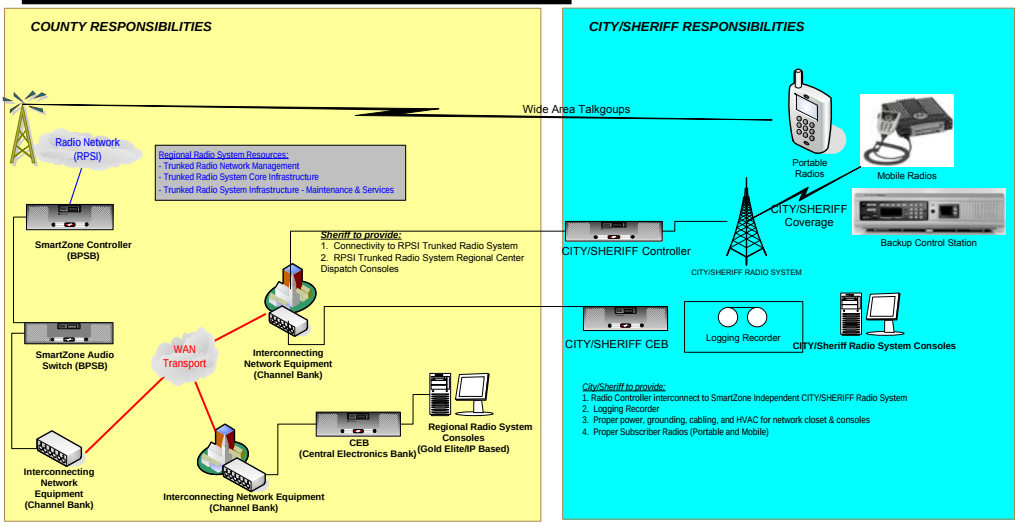
RPSI – Trunked Radio System
Logical Network Design Overview Broward County Radio System
Broward County/Sheriff/City Responsibilities



COUNTY – RADIO – ILA: Trunked Radio System – Direct Subscribers | Sheet 5 of 7

Broward County Radio Network: ILA Radio Demarc – Indirect Subscribers

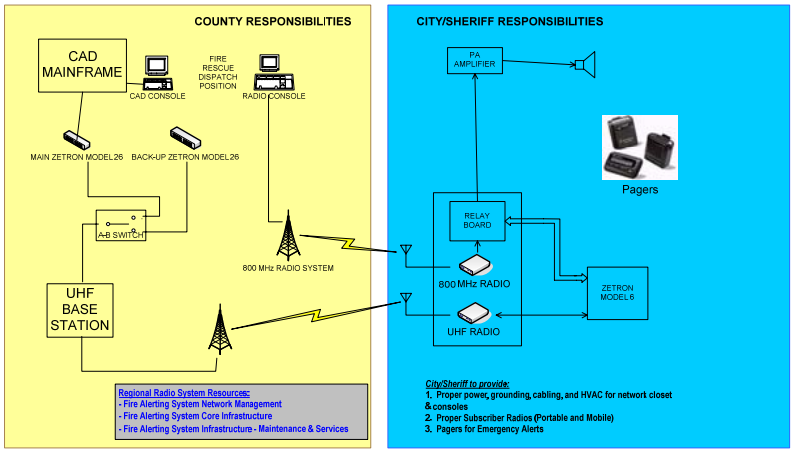
RPSI – Trunked Radio System
Logical Network Design Overview Broward County Radio System
Broward County/Sheriff/City Responsibilities



COUNTY – RADIO – ILA: Trunked Radio System –Indirect Subscribers | Sheet 6 of 7

Broward County-Station Alerting: ILA Fire Station Alerting System Demarcation Drawing

RPSI – Fire Station Alerting System
Logical Network Design Overview Broward County Radio System
Broward County/Sheriff/City Responsibilities



COUNTY – STATION ALERTING – ILA: Regional Fire Station Alerting | Sheet 7 of 7

EXHIBIT “C”

Equipment List

Model numbers are provided for reference only in this proposal and are subject to change.

EXHIBIT D

Change Management Request Procedure

Broward County
Office of Communications Technology

Change Management Request Procedure

Introduction

This document defines the Change Management Request (CMR) process for any component(s) that make up the Regional Public Safety Intranet providing delivery of services to end-users. The CMR process will be used to specify the times and conditions when designated tasks can be performed as maintenance on all software and equipment affiliated with the Regional Public Safety Intranet including but not limited to the Public Safety Network (PSN), Trunked Radio System, Computer Aided Dispatch (CAD) System, BI Query, PMDC, UDT/DSS, E-911, etc.

Objective

The objective of the CMR process is to implement maintenance and expansion guidelines that will assure system reliability; minimize the impact on end-users and prevent unintended outage conditions.

Definition

The CMR process will be an ongoing activity involved with the scheduling, communication and coordination of maintenance and construction activities impacting the RPSI. This process includes a Request, Review and Approval process. All change and maintenance activities are performed during predetermined and mutually acceptable Maintenance Windows.

Scope

The CMR process should be followed for any installation, equipment and software maintenance activity or any construction activity which either directly or indirectly impacts the Regional Public Safety Intranet.

CMR Process Requirements

All scheduled change and maintenance activities will require completion of an electronic CMR form and must conform to the following criteria:

- All work requests that impact directly or indirectly the end-users of Public Safety Mission Critical applications must be thoroughly documented in the CMR forms and sent as an e-mail attachment to: changemanagement@broward.org

- COUNTY's Office of Communication Technology (OCT) will review all requests and obtain consensus from Operations and from all impacted end-users on scheduling the Maintenance Window for the request.

- Activities will be scheduled and performed only during predefined or mutually acceptable Maintenance Windows.

- The Requestor submitting the Method of Procedure (MOP) form must identify the scope of the associated outage and a best estimate of the duration of the activities involved in the project. Stop times must take into account the time needed to restore the system to an operational state.

- Following COUNTY OCT approval of the submitted Method of Procedure (MOP), a project coordination meeting involving representatives of all involved or impacted parties will be scheduled by the assigned OCT Program Manager prior to the start of the scheduled work.

MOP Requirements

- The MOP must clearly state the objective(s) of the work to be performed; the parties performing the work; the parties impacted by the work and the steps to be completed by each party.

- A Maintenance Window identifying a clear Start and Stop time and a work flow schedule must be developed and included as part of the MOP.

- The scheduled work must follow the predetermined schedules identified in the MOP, and, as previously noted, stop times must take into account the time needed to restore the system to an operational state.

- The MOP must clearly identify the Program Managers responsible for coordination of the activity and provide telephone numbers and any other relevant contact information.

- The MOP must include an escalation list with notification time frames should unforeseen problems occur that would result in an outage extending beyond the scheduled Maintenance Window.

- The MOP must include a fallback plan should the original plan not work.

Emergency Maintenance

Emergencies by their nature are not a part of the CMR process, but can seriously impact end-users and any scheduled maintenance activities.

In the event of an emergency outage, both the affected end-user and first responder must notify the designated on-call person for the Office of Communications Technology (OCT). An on-call list will be provided to each

911/Dispatch Center Duty Officer and Manager. The OCT contact will be responsible for the following actions:

- Identifying and assigning resources to work the emergency.

- Acting as a liaison between the maintenance provider and the 911/Dispatch Center Duty Officer and Manager for the duration of the outage or service degradation.

- Documenting response times and actions taken, followed by generating an after-action report.

The maintenance provider(s) responding to an outage or service affecting emergency must take the following measures following notification:

- Upon notification, use remote access to diagnose and repair the problem or arrive on site within the contracted time frames of the responder's maintenance agreement.

- Assess the nature and scope of the problem.

- Notify the COUNTY OCT on-call person of all actions to be taken and provide the best possible estimate of the duration of the outage or service degradation.

- Notify the COUNTY OCT on-call person of any break in maintenance activity prior to completion of the repair for any reason.

- Provide periodic updates for extended outages.

- Document each step of the repair/troubleshooting process as it is performed.

- Within 24 hours of completion of a repair, provide a written summary of the problem and the measures taken to repair the problem and (if relevant) prevent similar future outages.

- COUNTY OCT managers will review the submitted documentation and on a case by case basis schedule a debriefing session to review the steps taken to resolve the problem and suggest changes or improvements for responding to future unscheduled outages.

Maintenance Windows

- The standard weekday Maintenance Window for Public Safety Communications Operations is 12:01 AM – 06:00 AM Sunday through Thursday or as otherwise specified by the Operations managers.

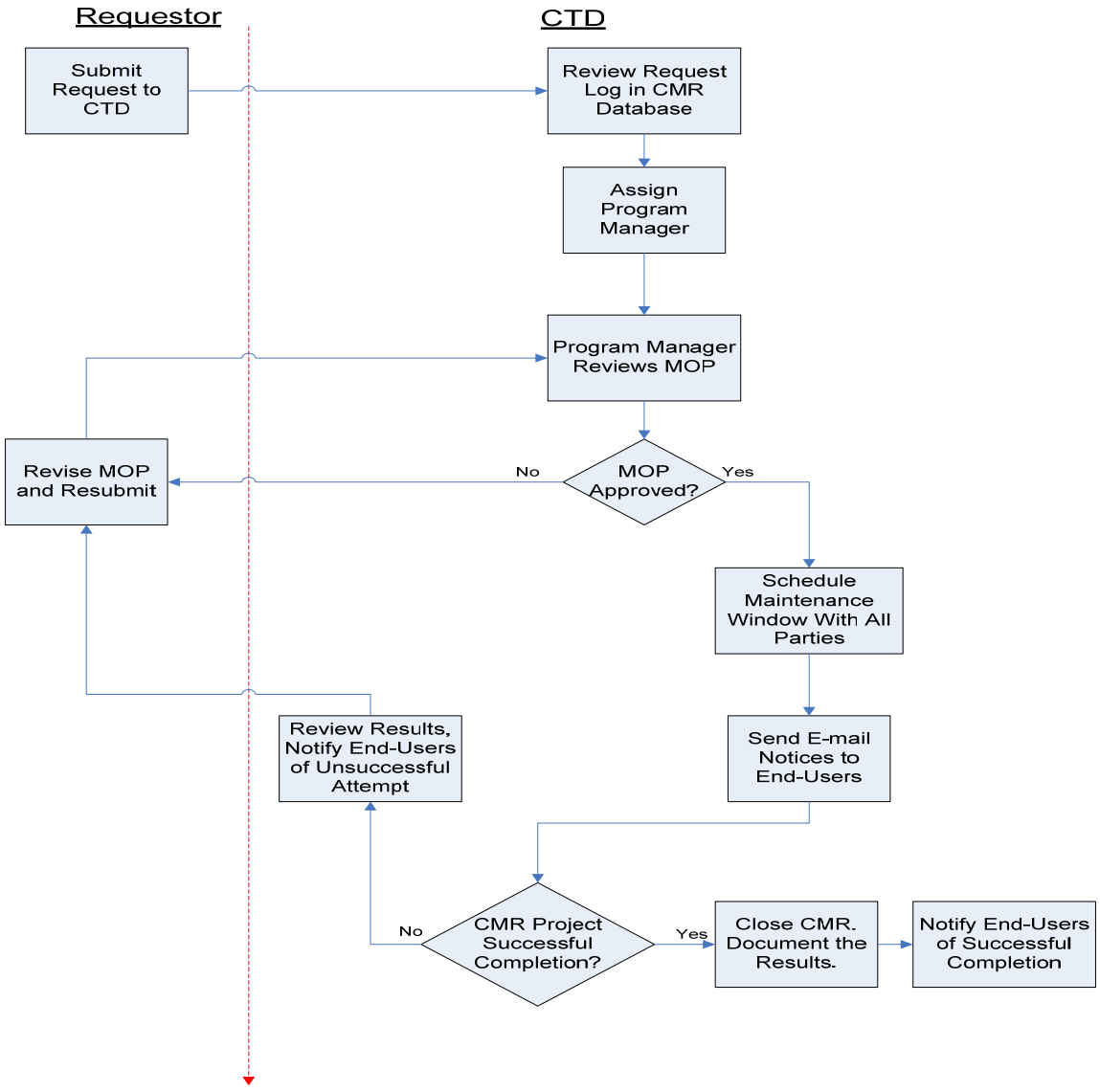
- The standard weekend Maintenance Window for Public Safety Communications Operations is 5:01 AM – 02:00 PM Saturday and Sunday or as otherwise specified by the Operations managers.

- A CMR must include sufficient time to perform a back-out of the change within the Window timeframe and restore systems to their normal operational state.

- A CMR that requires work to be performed outside the standard Maintenance Windows must include justification for performing the work during a non-standard window and be approved by COUNTY's OCT.

Change Management Request

Process Work Flow



Type	Risk Impact Level	Definition	Lead Time	MOP Required	Actions Description
FYI	**Non-Service Affecting**	**Prep work activity which has low risk to end-users of Public Safety Mission Critical applications.**	**Minimum 2 days**	**No**	**FYI as needed.**
Scheduled	**Potential-Service Affecting**	**Any activity that may impact end-user access to Public Safety Mission Critical applications.**	**Minimum 5 days**	**Yes**	**Notify all End-Users and Support Management**
Scheduled	**Service Affecting**	**Includes any activity which will result in the loss or degradation of accessibility to end-users of one or more Public Safety Mission Critical applications.**	**Minimum 10 days**	**Yes**	**Obtain written or e-mail approval from Management.** Provide Written Notification to all affected End-Users. Obtain Written Approval of all affected End-Users.
Scheduled	**Outage Required**	**Any work which will necessitate a total outage of one or more of the Public Safety Mission Critical applications or the Public Safety Wide Area Network, or any extremely high risk activity which may inadvertently cause an outage.**	**Minimum 10 days**	**Yes**	**Obtain written or e-mail approval from Management.** Provide Written Notification to all affected End-Users. **Obtain Written Approval of all affected End-Users.**
Emergency	**Service Affecting or Outage Required**	**The unscheduled outage of one or more Public Safety Mission Critical applications or the Public Safety Wide Area Network.**	**None**	**No**	**Requires immediate management and End-User notification and a debriefing meeting once the problem has been resolved.**

End-User Notification

Not less than ten (10) business days prior to an approved CMR project affecting the Regional Public Safety Intranet, the COUNTY OCT project manager must notify all end-user management by e-mail of the pending activity with all CMR and MOP documentation attached. The e-mail should summarize the attached documentation but must include:

- A list of all affected end-users.
- A generic statement of nature of upgrade or maintenance procedure and the operational need to make the change.
- The Maintenance Window, date and time the work will be performed including the projected end time.
- A generic impact statement that identifies the nature of the work being performed; the impact of the work on the end-user while the work is performed and the effect of the work on the restored system or application.
- Telephone numbers of project managers and key staff involved in the activity.

Approval Authority

Any and all activities being performed must be supported by an approved CMR document.

Broward County

Office of Communications Technology

Change Request Form

Note: Complete and submit to the Office of Communications Technology at Change_Management@broward.org. All Change Requests submitted prior to Wednesday are reviewed during the Thursday morning conference calls and either approved or returned for modifications. Please allow a minimum of ten (10) business days from the date of approval for your Maintenance Window to be scheduled. Any work performed on the Public Safety Communications Network, its supporting infrastructure, or the application servers must be documented and approved in a CMR.

Today's Date and Time:	
Requestor Name:	
Requestor Company Name or Agency:	
Requestor E-Mail:	
Requestor Phone Number:	Office:
	Mobile:
Briefly describe the Work to Be Performed:	
Identify End-Users & sites impacted by the work to be performed:	

What is the expected and desired end result of the Work to be Performed?	
Identify any loss or degradation of functionality and the impact on end-users during the Maintenance Window:	
Identify your On-Site Contact during the scheduled Maintenance Window:	Name & Contact Number:
Requested Maintenance Window for Work to be Performed:	Start Date & Time: Stop Date & Time:
Approved Maintenance Window for Work to be Performed:	Start Date & Time: Stop Date & Time:
Maintenance Window Approved By:	Date:
Assigned MOP Tracking Number:	

Method of Procedure – for Primary Contractor or Service Provider

Note: An MOP must be completed for each Contractor or Service Provider working on a specific project. Use electronic attachments as needed.

Company or Agency Name:	
Project Manager Name:	
Project Manager Office Phone Number:	
Project Manager Mobile Phone Number:	
Project Manager E-Mail:	

Detailed Project Description

Specify each step in the MOP Work Process. Attach additional pages or any supporting documents as needed:	
Describe back-out and restoration plans if stated project goals are not achieved within the allotted Maintenance Window:	

<table>
<tr><td colspan="3">OCT to complete Items 1 through 10 Below:</td></tr>
<tr><td colspan="2" rowspan="3">(1) OCT Contact for Project:</td><td>(2) Name:</td></tr>
<tr><td>(3) Mobile Phone Number:</td></tr>
<tr><td>(4) E-Mail:</td></tr>
<tr><td rowspan="5">(5) MOP Type:</td><td colspan="2">(6) FYI – Non-Service Affecting: ☐</td></tr>
<tr><td colspan="2">(7) Scheduled – Potential Service Affecting: ☐</td></tr>
<tr><td colspan="2">(8) Scheduled – Service Affecting: ☐</td></tr>
<tr><td colspan="2">(9) Scheduled – Outage Required: ☐</td></tr>
<tr><td colspan="2">(10) Emergency: ☐</td></tr>
<tr><td colspan="3">Reviewer Comments:</td></tr>
<tr><td colspan="2">Method of Procedure Approved By:</td><td>Date Approved</td></tr>
</table>

EXHIBIT "E"
Project Charter

PROJECT CHARTER

1. General Project Information

Project Name:		
Department/Agency Sponsor:		
• ***What department is the primary proponent of this project? (*Enter one.*)***		
• Who, within that department, is the Project Sponsor?		
• Is this a Regional Project, i.e. does it have significant impact on regional applications or resources (Y/N)?		
Department Co-Sponsor:		
Department/Agency Project Rank:		
If this project is mandated or is required for continued business operation:	**Mandated by whom?**	
	Impact of not meeting mandate?	

Document History

Version	Date	Author	Reason for Change
*	*	*	*

2. Stakeholders

	Name	*Department*	*Telephone*	*E-mail*
Project Manager:				
Tech Lead:				
Agency Lead:				
Others *(those with a significant interest in this project)*:				

2. Stakeholders

	Name	*Department*	*Telephone*	*E-mail*

3. Vendor Contacts

Name	*Company / Role*	*Telephone*	*E-mail*

4. Project / Service Description

Project Purpose / Business Justification

Objectives

Deliverables

Clear Statement of What This Project Will Not Include

Project Success

Project Milestones

Major Known Risks (including significant Assumptions)

Risk Rating (Hi, Med, Lo):
List the most significant risks to the project:
1.

Constraints

4. Project / Service Description

External Dependencies

Project Strategy

5. Financial / Resources Information

Funding Source *Select one of the following:* **Operating Budget, Capital Budget, Grant, Other**. *(If Other, please provide a description)*

Estimate of Implementation Cost

Implementation Cost: $

*Estimate time required of Multi-Department Staff (*Add rows as needed*)*

Role	Hours needed

*Estimate time required of other Organization Staff (*Add rows as needed*)*

Role	Hours needed

6. Estimated Total Cost of Ownership (TCO) 5-Year

*In the **Calendar/Fiscal Year** column, change years as approriate.*

*In the **Capital** and **Operational** columns, click on each entry once to select the full field (0.00) completely before entering the dollar figure.*

*In the **Totals** row, total the dollar figure in each column by placing the cursor on dollar figure field, clicking once to select it, then clicking the right mouse button and selecting Update Field.*

Calendar Year (1, 2, 3) or Fiscal Year (2004-5, 2005-6)	Capital ($U.S.)	Operational ($U.S.)
2007-8	0.00	0.00

2008-9	0.00	0.00
2009-10	0.00	0.00
20010-11	0.00	0.00
20011-12	0.00	0.00
Totals	***0.00***	***0.00***

7. Sourcing Strategy

Place an X in the appropriate adjacent box:

Organization-Managed and Hosted			**Sole-Source / Amend Contract**		
Vendor-Managed and Hosted			**RFP / Competitive Bid**		
Organization-Managed, Vendor-Hosted			**In-House / Custom-Develop**		
Vendor-Managed, Organization-Hosted			**Other:**		

Acquisition Strategy

Place an X in the appropriate adjacent box:

8. Types of Vendor Assistance

Place an X in the appropriate adjacent box:

Turnkey Solution			**Supplemental Staffing (Time/Materials)**		
Vendor-Assisted (Fixed Price)			**Hardware / Software**		
Other:			**None / Not Applicable**		

9. Sign-off

	Name	Title	Signature	Date (MM/DD/YYYY)
Business Sponsor				
Project Manager				
Customer A				
Customer B				
Customer C				
Customer D				

10. List of Addenda

List all files supplemental to this Charter here.

Document Name	Filename and Location

11. Notes / Comments

EXHIBIT "F" – ATTACHMENT 1
Service Level Agreements
Terms and Conditions

INTRODUCTION

This purpose of this Service Level Agreement (SLA) is to clarify the mutual expectations of the SHERIFF and the COUNTY. Changes in software and hardware architecture make it imperative that all members understand their mutual responsibilities.

1.0 MAINTENANCE SERVICE AND SUPPORT

1.1 Maintenance Service and Support being provided are based on the Severity Levels as defined below. Each Severity Level defines the actions that will be taken by COUNTY for Response Time (MTTR), Resolution Time, and Resolution Procedure for reported errors. Response Times for Severity Levels 1 and 2 are based upon voice contact by SHERIFF, as opposed to written contact by e-mail, facsimile or letter. Should delays by SHERIFF prevent scheduling of downtime to resolve an issue, COUNTY will not be held responsible for Resolution time frames listed below.

SEVERITY LEVEL	DEFINITION	MTTR (Mean Time To Respond)	TARGET RESOLUTION
1	Failure/Outage occurs when the system is not functioning which prohibits continuance of mission critical operations.	≤30 minutes of initial voice notification*	Resolve within 24 hours of initial notification*
2	Failure occurs when an element in the system is not functioning that does not prohibit continuance of normal daily operations.	≤ 24 business hours of initial voice notification.*	Resolve within 5 standard business days of initial notification*
3	An Inconvenience occurs when software or hardware causes a minor disruption in the way tasks are performed but does not stop workflow.	≤48 business hours of initial notification	Resolution determined on a case by case basis.

*Does not apply to "READ-ONLY" CAD Systems

1.2 The SHERIFF System Administrator shall conduct a preliminary error review to verify a problem, determine if such is the direct result of a defect in Hardware, Software, or other and the direct conditions under which the problem occurred, identify the applicable urgency rating scale by which errors, problems, and other issues are scheduled ("Severity Level"), and ascertain that errors are not due to an external system, data link between systems, or network administration issue prior to contacting COUNTY.

1.3 SHERIFF shall assign an initial Severity Level for each error reported, either verbally or in writing, based upon the Severity Levels defined above. Severity Level 1 or 2 problems should be reported verbally to the COUNTY by SHERIFF Representative or System

Administrator. COUNTY will notify the SHERIFF if COUNTY makes any changes in Severity Level (upgrade or downgrade) of any SHERIFF-reported problem.

1.4 COUNTY shall provide telephone support for maintenance issues 24 hours per day, 7 days a week (24 x 7).

1.5 All requests for support for the products specified in this Exhibit will be logged with the COUNTY Customer Support Center ("CSC") via telephone at 1-954-357-8570 or email at ctdsupport@broward.org

1.6 COUNTY will provide SHERIFF with a resolution within the appropriate Resolution Time and in accordance with the assigned error Severity Level when COUNTY diagnostics indicate that the error is present. Additionally, COUNTY will verify: (a) the Hardware and Software operates in conformity to the System Specifications, (b) the Hardware and Software is being used in a manner for which it was intended or designed, and (c) that the Hardware and Software is being used only with COUNTY approved Hardware or Software. Resolution Time period shall not begin to run until such time as the verification procedures occur. COUNTY will continue to provide service support under this Inner Local Agreement until final resolution is determined.

1.7 Should COUNTY determine that it is unable to correct such reported error within the specified Resolution Time, COUNTY will upgrade and escalate its procedure and assign such personnel or designee to correct such error. This will include automatic problem call escalation to appropriate levels of COUNTY Management.

1.8 Any and all Maintenance Service provided for herein shall be warranted under the following terms and conditions:

a) Third party hardware, software, and any other related supplies shall conform to any and all applicable industry approved technical, functional, and performance specifications;

b) The System is free of modifications and alterations which have not been pre-approved by COUNTY.

c) The System is free of any evidence of negligence, misuse and/or abuse, intentional or otherwise.

1.9 Unless otherwise specified herein, any and all suspected errors will be investigated and corrected at COUNTY Facilities. COUNTY shall decide whether on-site correction of any Hardware and Software error is required.

1.10 Any third party equipment supplied by COUNTY shall be guaranteed by the manufacturer's warranty for that equipment.

2.0 RECORD –KEEPING AND REPORTING RESPONSIBILITIES

2.1 COUNTY will provide verbal and written status reports on Severity Level 1 troubles. Written status reports on outstanding errors will be provided to SHERIFF System Administrator on a monthly basis upon request.

2.2 COUNTY shall provide annual account reviews to include: a) service history of site; b) downtime analysis; and c) service trend analysis.

2.3 COUNTY will prepare the following reports (for PremierCAD software only), to include:

a) System Analysis	MEASURE:	Evaluate disk and CPU load
	PEEK:	Evaluate memory availability and use
	VIEWSYS:	Evaluate use and availability of PCBs
	EMSA/TMDS:	Review logs for hardware reports
	File Sizing:	Review file sizing on changeable files

b) Pathway Analysis Evaluate effectiveness of system configuration for current load.

Evaluate TCP/Server statistics.
Evaluate efficiency of server class maximum and minimum settings.

c) Performance Analysis TMX Timings: Evaluate application response times

d) Printrak Technical Support Analyst. Based on the Annual System Performance Review and Reports, the Printrak Technical Support Analyst will review findings and recommend software or hardware changes to improve overall operations.

3.0 MISCELLANEOUS

3.1 When COUNTY performs service at the System location, SHERIFF agrees to provide COUNTY, at no charge, a non-hazardous environment for work with shelter, heat, light, and power and with full and free access to the System.

3.2 SHERIFF will provide all information pertaining to the SHERIFF owned hardware and software elements of any equipment with which the System is interfacing that enable COUNTY to perform its obligations under this Service Agreement.

3.3 It is not required that parts furnished by COUNTY be newly manufactured. COUNTY warrants such parts to be equivalent to new in performance. Parts replaced in the course of repair shall, at the close of maintenance, become COUNTY's property.

3.3 SHERIFF will provide a qualified System Administrator for the Printrak System Portion to perform all functions as defined in Printrak's Systems Administrator's guide which has been provided to the SHERIFF under separate cover.

3.4 Upon the expiration or earlier termination of this Agreement, SHERIFF and COUNTY shall immediately deliver to the other Party, as the disclosing Party, all Confidential Information of the other, including any and all copies thereof, which the other Party previously provided to it in furtherance of this Agreement. Confidential Information shall include: (a) Proprietary materials and information regarding technical plans; (b) any and all other information, whether in a softcopy or hardcopy medium, including but not limited to data, developments, trade secrets and improvements that is disclosed in any form by COUNTY to SHERIFF; (c) all GIS, address, telephone, or like records and data provided by SHERIFF to COUNTY that is required by law to be held confidential.

3.5 This Service Level Agreement does not grant directly, by implication, or otherwise, any ownership right or license under any patent, copyright, trade secret, or other intellectual property including any intellectual property created as a result of or related to the products sold or Services performed under this Service Level Agreement.

4.0 SOFTWARE UPDATES

COUNTY shall provide software updates as defined below:

4.1 Supplemental Release is defined as a minor release that contains primarily error corrections to an existing Standard Release. It may also contain limited improvements that do not affect the overall structure of the Software. Supplemental Releases can be installed remotely. Supplemental Releases are identified by the third digit of the three-digit release number, shown here as underlined: "1.2.3".

4.2 Standard Release is defined as a major release of Software that contains product enhancements and improvements such as new databases, modifications to databases, new server/requesters, etc., and may involve file and database conversions, System configuration changes, hardware changes, additional training, modifications of Software license terms, on-site installation, and System downtime. Standard Releases are identified by the second digit of the three-digit release number, shown here as underlined: "1.2.3".

4.3 Product Release is defined as a major release of Software considered to be the next generation of an existing product or a new product offering. Product Releases are identified by the first digit of the three-digit release number, shown here as underlined: "1.2.3".

4.4 At SHERIFF's request, COUNTY will provide a current list of compatible hardware operating system releases. A list of Software Supplemental or Standard Releases will also be made available at no charge to SHERIFF.

4.5 SHERIFF must maintain all hardware and software connected to the COUNTY's network to the latest compatible revisions.

5.0 ADDITIONS AND CHANGES

5.1 The SHERIFF may request an enhancement to System functionality. Enhancement requests are submitted to COUNTY Office of Communications Technology (OCT) for review. If OCT accepts the enhancement request, request will be referred to the Program Management Team for possible inclusion in a future project. OCT will provide a response to the enhancement request within ninety (90) standard business days upon written receipt of initial request. If accepted, a proposed Project Plan will be furnished with any applicable enhancement fee. The SHERIFF may choose to pay for an enhancement request that has been accepted by Program Management but is not viewed as a high enough priority to include in a release.

6.0 ACCESS

6.1 The SHERIFF agrees to maintain any and all electrical and physical environments in accordance with System manufacturer's specifications.

6.2 The SHERIFF agrees to ensure System accessibility, which includes physical access to building as well as remote access. Remote access is required and will not be substituted with on-site visits if access is not allowed or available.

7.0 EXCLUSIONS

7.1 Maintenance Service and Support not listed in this SLA are excluded, and COUNTY shall not be liable under this Agreement for such services. Exclusions consist of, but are not

limited to:

a) Any service work required due to incorrect or faulty operational conditions, including but not limited to equipment not connected directly to an electric surge protector, equipment used in a non-office environment, and equipment not properly maintained in accordance with guidelines set forth in the manufacturer's User's Guide;

b) The repair or replacement of parts resulting from failure of the SHERIFF's facilities or SHERIFF's personal property and/or devices connected to the System (or interconnected to devices) whether or not installed by COUNTY's representatives;

c) The repair or replacement of Equipment that has become defective or damaged due to physical or chemical misuse or abuse from causes such as lightning, power surges, or liquids;

d) The repair or replacement of any transmission medium, such as telephone lines, computer networks, or the worldwide web, or for Equipment malfunction caused by such transmission medium;

e) Accessories; custom or Special Products; office furniture which includes chair(s) and workstation(s); modified units; or modified software;

f) The repair or replacement of parts resulting from the tampering by persons unauthorized by COUNTY or the failure of the System due to extraordinary uses;

g) Operation and/or functionality of SHERIFF's personal property, equipment, and/or peripherals and any non-COUNTY provided application software including service of any accessory, attachment, or component owned by SHERIFF, whether or not installed by COUNTY;

h) Removal, relocation, and/or reinstallation of System or any component thereof;

i) Services to diagnose technical issues caused by the installation of unauthorized components or misuse of the System.

j) Operational supplies including, but not limited to, printer paper, printer ribbons, toner, photographic paper, magnetic tapes, any supplies in addition to that delivered with the System, and battery replacement for uninterruptible power supply (UPS).

k) Unauthorized installation of any Software or Hardware modifying Printrak Software and/or the System.

7.2 SHERIFF shall be responsible for payment of any desired service and support not included within the scope of this SLA and such service or support shall be performed at the rates set forth below.

Billable rates are subject to a two (2) hour minimum:

$100 per hour	8 a.m. – 5 p.m. (local time) Monday – Friday
$150 per hour	After 5 p.m. Monday – Friday, and all day on Saturday, Sunday and COUNTY established holidays
Travel Expense	In addition to the above hourly labor rates, all other actual travel related expenses may be charged to SHERIFF.

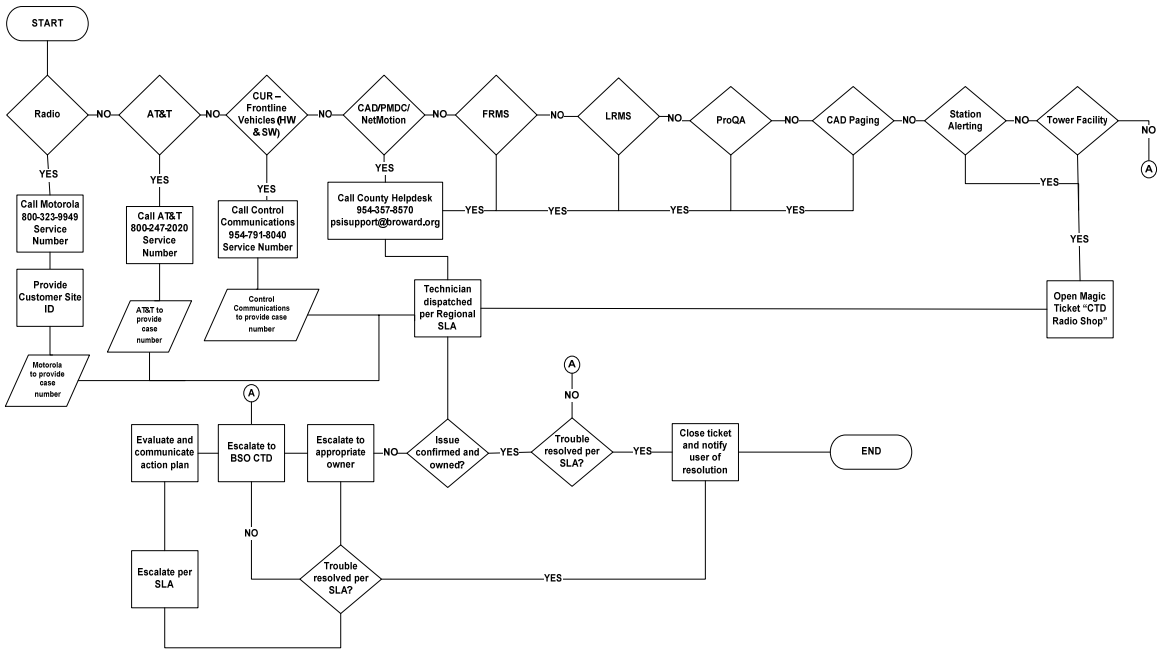
LIST OF HARDWARE and SOFTWARE

The following lists the System hardware and software items under the ILA coverage/control of COUNTY's area of responsibility:

EXHIBIT "F" – ATTACHMENT 2
Service Level Agreements
Trouble Ticket Workflow

RPSI: Interlocal Agreement Trouble Ticket Workflow

Broward County Communications Technology Division - Public Safety Intranet



- Note 1: All Severity 1 Cases are to be escalated to Broward County CTD.
- Note 2: Radio Support assumes CITY/SHERIFF has a current maintenance contract with Motorola.
- Note 3: CITY/SHERIFF may have current maintenance contract for station alerting.

* BROWARD COUNTY CTD CONFIDENTIAL AND PROPRIETARY *

RADIO / PUBLIC SAFETY APPS TROUBLE REPORTING WORK FLOW

Created by: Daniel Revis
Created on: 5/16/2007
Last edited by: Daniel K. Revis
Revision: 0
Last edited on: 9/13/2012
Sheet 1 of 1

EXHIBIT "G"

Trunked Radio System
Standard Operating Procedures

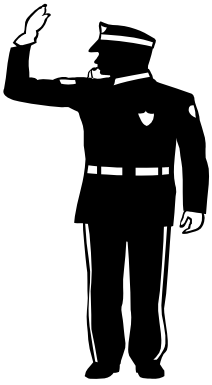
Regional Public Safety

Communications –

Radio Sub-Committee

Standard Operating Procedures

For the Broward County Public Safety Intranet



RPSCC RADIO SUB-COMMITTEE

STANDARD OPERATING PROCEDURES

FOR THE BROWARD COUNTY

PUBLIC SAFETY INTRANET

TABLE OF CONTENTS

SOP #	PROCEDURE TITLE
1.1	Fleetmap Standards
1.2	Talk Group & Radio User Priority
1.3	Telephone Interconnect
1.4	Private Call
1.5	Radio Aliases
1.6	Radio Model and Features
1.7	Radio Auxiliary Equipment
1.8	Talk Group Names
1.9	Shared Use of Talk Groups
1.10	Scanning Talk Groups
1.11	Emergency Button
1.12	Encryption
1.13	Definitions & Acronyms
1.14	Console Naming

STANDARD OPERATING PROCEDURES (SOP)

800 MHz Trunked Regional Public Safety Radio System
Standards, Protocols, Procedures

Document Section: 1.1 Sub-Section: Procedure Title: **Fleetmap Standards** Date Established: 12/15/06 Replaces Documents Dated: N/A Date Revised: N/A	RPSCC Radio Sub-Committee Approved Date: 08/02/07

1. Purpose or Objective:

The 800 MHz system will contain a large number of talk groups & multigroups to support the various agencies that will be subscribing to the system.

The System has multiple administrating agencies that will be responsible for maintaining the Fleetmaps and system programming for the agencies for which they are responsible.

Talk groups must be configured identically by name in the SmartZone Manager Terminal database, Radio Consoles and the Subscriber Radio. The minimum characters are six (6) and maximum is 14. The Talk Group number of characters will need to be based upon the individual agency's subscriber radio model types used within their fleet.

For the effective management of the system a defined process needs to be used to document the Fleetmap information that each agency is supporting. This information needs to be in a format that is shared with the other administrators.

2. Technical Background:

- **Capabilities:**

The Fleetmap is parameter information programmed into the system infrastructure and into the subscriber radios to control how the radios will behave on the 800 MHz system.

The Fleetmap itself contains the following information:

Fleetmap Information	Definition
Talkgroup	Name of the talkgroup & multigroup as it is programmed into the system
Talkgroup ID	Numerical ID of the talkgroup & multigroup
Owner	The actual "owning" agency of the talkgroup
Description	General description of the talkgroup & multigroup
Multigroup	If the talkgroup is part of a multigroup, this will identify the multigroup
Priority	Priority level of the talkgroup
Admin Agency	The agency that is responsible for the system administration for this talkgroup
Site # access	Will be a listing of the RF sites individually, and if the talkgroup is authorized
Media Access	If media access is permitted for this talkgroup
Global Sharing	The predefined global sharing authorizations

User Groups = The subscriber groups using the talk groups, this becomes a matrix for programming.

The Fleetmap spreadsheet will become a documented matrix of the talk groups in the system and the subscriber groups that are using / sharing these talk groups.

3. Operational Context:

The System Managers will be responsible for managing the Fleetmap information of the users they are representing. This information is also shared with the other system managers; the ID information also must be kept.

4. Recommended Protocol/Standard:

The detailed matrix will be maintained on the system database. An example of the matrix layout is shown in this manual. ***Need to develop the matrix layout.***

Each System Manager will maintain a master Fleetmap spreadsheet containing data on the subscribers for whom they are responsible.

5. Recommended Procedures:

As individual System Managers make updates and changes to their spreadsheets, the spreadsheet will be e-mailed to the Broward County COUNTY's Office of Communications Technology Radio Communications Manager, the Administrator (for future reference this person will be

referred to as the “Primary Administrator”) of the system. This will allow the Primary Administrator to update the master spreadsheet information easily and provide the information to the other System Managers for reference and integrity of the Fleetmap planning process.

Talk groups that are shared between subscribers of different administrating agencies will be reflected on all the spreadsheets having subscribers using these talk groups. The portion of the System Manager’s spreadsheet containing data on talk group ownership will be considered the master reference for the Talk group.

The disclosure of the Fleetmap configuration information including Talk Group IDs, user IDs, user privileges and other related system information would substantially jeopardize the security of the system from tampering, sabotage, unauthorized use, jamming, hacking, unauthorized access to the contents of confidential voice and data communications, etc. Therefore, the master Fleetmap spreadsheets shall be classified as “Security Information” and “Non-Public Data.” The System Managers may choose to disclose some or all of their own information to their users; however, they shall not disclose other Agencies’ information without prior approval from the responsible System Manager.

6. <u>Management</u>:

The System Managers Group will manage the Fleetmap information and the details of the process for communicating the information.

Standard Operating Procedures (SOP)

800 MHz Trunked Regional Public Safety Radio System
Standards, Protocols, Procedures

Document Section: 1.2 Sub-Section: Procedure Title: **Talk Group & Radio User Priority** Date Established: 12/15/06 Replaces Document Dated: N/A Date Revised: N/A	RPSCC Radio Sub-Committee Approved Date: 08/02/07

1. Purpose or Objective:

The purpose of establishing varying priority levels for talk groups is to assure the most critical talk groups on the system are granted a channel as quickly as possible when the system is experiencing busy conditions.

2. Technical Background:

- **Capabilities**

  The system priorities can be managed at the user level and at the Talk Group level.

- **Constraints**

  All User Priorities will be set at 10, as radio users change talk groups, their effective priority will be set by the Talk Group that they are on.

3. Operational Context:

Priority levels in the system will be managed at the Talk Group level. The goal is to distribute priorities across the systems talk groups in a way that maximizes the ability for critical groups to communicate and minimizes the number of talk groups with high priority. All User Priorities will be set to the lowest priority level, 10.

4. Recommended Protocol/Standard:

The Talk Group owner, or the applicable subsystem owner, shall assign Talk Group priority levels not exceeding the level defined by the criteria below. Talk Group priorities that are assigned to level five or above are subject to the review and audit of the RPSCC Radio Sub-Committee.

Priority 1 Definition – EMERGENCY: Only Emergency Alert calls, i.e. emergency button pressed, will be given the Priority 1 status. Definition of an EMERGENCY means when a public safety radio subscriber encounters a life-threatening situation and needs help by activating their emergency button which then activates their designated dispatcher's radio console with an emergency alert.

Priority 2 Definition – Unassigned

Priority 3 Definition – Unassigned.

Priority 4 Definition – Public Safety Talk Groups

Priority 5 Definition – Low Priority Public Safety Talk Groups

Priority 6 Definition – Unassigned

Priority 7 Definition – Local Government Essential

Priority 8 Definition – Unassigned:

Priority 9 Definition – Local Government Non-Essential

Priority 10 Definition – PRIVATE & INTERCONNECT CALLS: Will be used for Telephone Interconnect Calls, Private Calls as defined by direct point-to-point or radio-to-radio communications that are not carried out within a talk group. This priority will also be used for talk groups that are established for system testing.

5. Recommended Procedures:

N/A

6. Management:

The RPSCC Radio Sub-Committee is responsible for supervision and management of this procedure.

STANDARD OPERATING PROCEDURE (SOP)

800 MHz Trunked Regional Public Safety Radio System
Standards, Protocols, Procedures

Document Section: 1.3 Sub-Section: Procedure Title: **Telephone Interconnect** Date Established: 12/15/06 Replaces Document Dated: N/A Date Revised: N/A	RPSCC Radio Sub-Committee Approved Date: 08/02/07

1. Purpose or Objective:

To manage the use of interconnect on the system. Although this is a useful feature and needed by some users, it must be managed to an appropriate level to protect the primary radio communications purpose of the system.

2. Technical Background:

- **Capabilities**

  Interconnect calls can be placed to individual users of the system, if they are configured for interconnect functionality. Interconnect calls can be placed to talk groups of the system, if the Talk Group is configured for interconnect functionality.

  Interconnect is intended to be a BACKUP functionality to cellular communications and used primarily on an emergency basis.

- **Constraints**

  - An interconnect call will consume an RF channel for the duration of the call.
  - Interconnect calls are half duplex; only one end can talk at a time.
  - A type 1 portable cannot initiate an interconnect call.
  - A type 2 portable can only place calls to numbers that are pre-programmed into the radio.
  - A type 3 portable can place an interconnect call by dialing the number directly.
  - The general public can easily monitor the interconnect calls and they are NOT private or protected in any way.
  - Interconnect shall NOT be utilized to conduct confidential business such as discussing case strategy with the State Attorney's Office.

3. Operational Context:

If a radio user has a need for interconnect, it shall be granted, but the resources impact needs to be carefully managed. Due to the risk of cutting off emergency / life safety communications, the duration of interconnect calls shall be set to a time limit of two (2) minutes. Only one channel within a radio system will be allowed the feature of Telephone Interconnect. The need to make a Telephone Interconnect call must be restricted to emergency and business related use. The SHERIFF of Fort Lauderdale has two (2) channels available for the users that are allowed the Telephone Interconnect feature; however, they do not permit other agencies to utilize their Interconnect resources.

4. Recommended Protocol/Standard:

Interconnect usage shall only be programmed for the users of the system that have a need for the function, the primary purpose of the system is for radio communications, but there may be some users that may require a backup ability to cellular communications.

The priority level for interconnect calls is “10,” this is defined under the priorities standards documents.

The interconnect equipment of the system will be configured to use the “overdial” method of operation, where the incoming calls come into a generic phone number, and then the interconnect ID of the radio is entered to complete the call. The Fort Lauderdale radio system does not support inbound interconnection.

5. Recommended Procedures:

The System Managers need to define and manage the interconnect properties of the RF subsystem(s) that they are responsible for. Each RF subsystem can be configured individually for the number of calls that they will be allowed to simultaneously carry.

6. Management:

The System Managers shall be responsible for following this procedure and monitoring the effect and usage of this resource. If negative impact or excessive usage is determined, interconnect permission will be reconsidered and possibly revoked. Definition of “negative impact or excessive usage is defined as individuals who are reported for using this feature for non-emergency and/or non-business related matters.

STANDARD OPERATING PROCEDURE (SOP)

800 MHz Trunked Regional Public Safety Radio System
Standards, Protocols, Procedures

Document Section: 1.4 Sub-Section: Procedure Title: **Private Call** Date Established: 12/15/06 Replaces Document Dated: N/A Date Revised: N/A	RPSCC Radio Sub-Committee Approved Date: 08/02/07

1. Purpose or Objective:

To manage the use of private call on the system, although this is a useful feature and needed by some users, it must be managed to an appropriate level to protect the primary radio communications purpose of the system.

2. Technical Background:

- **Capabilities**

  Private calls can be placed to individual users of the system, this communication is outside of the Talk Group communications, and is a private communication between two radio users. Console operators can place private calls to the radio users.

- **Constraints**

  - A private call will consume a RF channel for the duration of the conversation.
  - Private calls are half-duplex, only one end can talk at a time.
  - A type 1 portable cannot initiate a private call.
  - A type 2 portable can only place private calls to numbers that are pre-programmed into the radio.
  - A type 3 portable can place a private call by dialing the number directly.
  - Private calls are not recorded.
  - For the duration that a radio user is involved in a private call, the user will not be involved in dispatch / Talk Group communications.
  - The system is not able to restrict the usage of private call on the system, unlike interconnect calls, which can be managed.

3. Operational Context:

The private call resource should primarily be used as a supervisory function, if

there is a business need for a radio user to have this ability, it should be granted, but the resource overall needs to be managed to protect the RF resources of the system. This is also a function that dispatch consoles overall would be capable of. Due to the risk of cutting off emergency / life safety communications, the duration of Private Calls must be set to a time limit of two (2) minutes. The number of channels that allow the feature of Private Call will be determined by the individual System Manager. The need to make a Private Call must be restricted to emergency and business related use. Radio users of the Private Call feature must understand that when this feature is being used, they cannot hear a Dispatcher call.

4. Recommended Protocol/Standard:

Private call usage will only be programmed for the users of the system that have a need for the function the primary purpose of the system is for radio communications. Site access for private call is managed in the "Sites Profile Group" that the radio user belongs to.

5. Recommended Procedures:

System Managers shall work with the user groups they are responsible for to plan the appropriate private call programming requirements for those users, in order to protect the RF resources of the system.

6. Management:

The System Managers shall be responsible for following this procedure and monitoring the effect and usage of this resource. If negative impact or excessive usage is determined, private call permission will be reconsidered and possibly revoked. Definition of "negative impact or excessive usage is defined as individuals who are reported for using this feature for emergency and/or non-business related matters.

STANDARD OPERATING PROCEDURES (SOP)

800 MHz Trunked Regional Public Safety Radio System
Standards, Protocols, Procedures

Document Section: 1.5 Sub-Section: Procedure Title: **Radio Aliases** Date Established: 12/15/06 Replaces Document Dated: N/A Date Revised: N/A	RPSCC Radio Sub-Committee Approved Date: 08-02-07

1. Purpose or Objective:

The purpose of this section is to set forth the principle by which all radio users in the regional system will establish names for their radios in order to ensure that there are no duplicate names, and also to facilitate intuitive understanding of the radio name.

2. Technical Background:

- Constraints

Every Radio User ID in the system has to be unique; there can be no duplicate IDs. The Radio User Alias field itself will hold up to 14 characters and the legal values that the system will accept are: Upper Case Alpha, Numeric, Period, Dash, Forward slash, Number sign.

When agencies make additions, deletions and changes to the database for Radio Aliases the modifications will not take affect until Motorola performs a database back-up that will occur every Friday. The Dispatch consoles will not reflect these modifications until that step is taken.

3. Operational Context:

With the exception of the first three (3) characters users are technically free to choose any unique name they wish for their radio aliases. However, since this is a shared system Radio User Aliases that are programmed into the system must have naming conventions between agencies that will not conflict with each other.

4. Recommended Protocol/Standard:

In order to meet this need the Radio User aliases would be prefixed with an agency identification that would be unique to that agency and would preferably readily identify the agency the Radio User is associated with. Because of the number of agencies using the system the prefix would be a minimum of two

alphanumeric characters in length in order to avoid contention between agencies.

Regional Operating Agencies and all agencies within the County of Broward would have naming prefixes of at least two digits that would stand alone. Counties would be pre-named with a two digit mnemonic, and the Cities and Agencies of the Counties would be included under the prefix of the County they are in.

Region 7 Operating Agencies and Broward County Region Agencies will have a naming prefix of at least two (2) letters that would describe their area. The naming standard only governs the first two characters; the characters following the first two are at the individual agency's discretion, for example; the agency may opt to internally use more than two characters for the internal identifications.

The following are suggestions for the body of the subscriber alias name. The body of the alias would contain an agency's identification for the individual or pool radio etc., possibly the radio user's call sign as an example. The alias could be suffixed with identification for the radio itself, such as a "-P" for portable for example to differentiate between a mobile & portable radio used by the same person. This would allow Dispatchers & System Managers to readily identify radio users and if the radio is a portable or a mobile.

Lost radios or radio IDs that are not associated with a radio user or console: A possibility for locating unused radios in the system that are lost, or not assigned to subscribers would be to temporarily prefix the radio serial number with a dash "-"at the time the radio is lost, or when the radio user is assigned to another radio. A report of these radios can be created by the SmartZone configuration reports tool and setting the radio selection criteria to "Radio Serial #," Start range -0, End range -999999.

A master list of Radio User Aliases will be created and maintained in the system. They will be readily accessible through the data terminal for all who have rights on that part of the system. As alias names are created and approved they will be placed on this master list so as to be available for all appropriate parties for operations and planning.

REGIONAL SYSTEM NAMING PREFIXES

2-3 Character Prefix	Name of the Agency using the Prefix
BC	Broward County Local Government
BCP	NPSPAC Mutual Aid
BCSB	Broward County SHERIFF
BSO	Broward COUNTY's Office Police and Fire Rescue
CC	Coconut Creek
CM	Communications – Joint Operations
CS	Coral Springs
DV	Davie
DB	Deerfield Beach Fire Rescue
DN	Dania Beach Fire Rescue
FL	Fort Lauderdale
FSO	Motorola Field Service Operation (FSO)
HB	Hallandale
HBB	Hillsboro Beach
HW	Hollywood Police, Fire Rescue and Local Government
LH	Lauderhill
LP	Lighthouse Point
MED	Broward County MEDCOM
MG	Margate
MM	Miramar
OP	Oakland Park
PB	Pompano Beach Local Government
PB	Pompano Beach Fire Rescue
PL	Plantation
PP	Pembroke Pines
SEM	Seminole Tribe
SN	Sunrise
WM	Wilton Manors

5. Recommended Procedures:

N/A

6. Management:

The System Managers are responsible for seeing that the defined standard is followed and maintained.

STANDARD OPERATING PROCEDURES (SOP)

800 MHz Trunked Regional Public Safety Radio System
Standards, Protocols, Procedures

Document Section: 1.6 Sub-Section: Procedure Title: **Radio Model and Features** Date Established: 01/04/07 Replaces Document Dated: N/A Date Revised: N/A	RPSCC Radio Sub-Committee Approved Date: 08/02/07

1. Purpose or Objective:

The purpose of this section is to set forth the recommended standards by which all 800 MHz radio users in the regional system will agree to purchase subscriber radios that are defined in this standard. This standard is to ensure that radios that are not in compliance do not affect the radio system. This document will be revised after the RPSCC approves the purchase and implementation of a new APCO P25 700 MHz radio system and the manufactured radio models have been identified to work with the P25 system.

2. Technical Background:

- **Constraints**

Radios must meet the recommended standards as set forth. These standards identify the proper radio to be used in conjunction with the required features and auxiliary equipment (to be described in Section 1.7) Each subscriber radio will be assigned it's unique Radio ID number, Alias Name and programmed with a codeplug/template that has been approved by the user's upper level management.

3. Operational Context:

All radios are programmed with the required Talk Groups, Mutual Aid (Local and Statewide) and features to allow it to operate on the 800 MHz Trunked radio system. Codeplugs/templates are created by the individual agencies radio shop or their contracted vendor.

4. Recommended Protocol/Standard:

In order to meet these requirements the following information describes the minimum standards that must be considered when new radios are purchased. Radios of various manufacturers and models are capable of operating on this

network. The Network currently consists of a Motorola SmartZone 3600 Baud Control Channel infrastructure. It is recommended that mobiles and portables be capable of operation with SmartZone features to permit the automatic roaming between sites as the users move out of range of their home system. SmartNet radios can be utilized where there is no intention of providing the automatic roaming features. With an eye to the future, where P25 and 700 MHz may be introduced, it is recommended that the subscriber units with a life expectancy past 2009 be either upgradeable or be equipped to operate on 700 MHz using the P25 protocol. For Public Safety users it is strongly recommended that the current Motorola products be utilized. System Managers can advise on the appropriate features, functionality and options to purchase. As a minimum, all radios shall have the ability to be assigned a unique individual ID number for system access, have the ability to be inhibited by command from the System Management tools and have an adequate talkgroup/channel capacity to permit the Local, Regional and National Mutual Aid talkgroups and channels to be programmed along with local agency requirements. The radios shall be capable of operating both in conventional mode and Motorola Trunking modes. There are other Trunking protocols that are not compatible, and radios utilizing these protocols shall not be authorized. These protocols include, but may not be limited to, Privacy Plus, EDACS, LTR and TETRA.

Mobile Radios shall have their power set to the lowest possible value. The radio systems in Broward County are designed to work in-building with portable radios. Constraints are placed upon the acceptable mobile radio power levels that should be utilized by this in-building design and the close spacing of the frequencies utilized by the network. Excessive power can cause undesired interference to the other users on the network. Older model radios shall be set to the lowest power permitted by their design, typically the half-power point. Non-Public Safety mobiles shall utilize 1/4 wave antennas, not gain style antennas.

Any Public Safety user that desires to utilize a high power setting for a specific System's Talk Groups shall obtain permission from the System Managers. The radios shall be programmed to power up in the low power mode and require a positive action on the part of the user to increase the power level. There shall be policies and procedures written to address the use of high power only after communications are unsuccessful when using the low power setting, and when working outside the primary coverage area of the network. If wide area talkgroups are involved, the totality of the wide area coverage, and not that of a more restricted coverage system, shall determine if high power usage is appropriate.

PORTABLE RADIO STANDARDS							
Model Description	**XTS2500 Model I**	**XTS2500 Model II**	**XTS2500 Model III**	**XTS5000 Model 1**	**XTS5000 Model II**	**XTS5000 Model III**	**XTS1500 Model I**
Digital	O	O	O	O	O	O	O

SmartZone	O	O	O	O	O	O	O
Dual Mode 800/700 MHz capable	S	S	S	S	S	S	S
Project 25 9600 SW	O	O	O	O	O	O	O
RF Switch (764-806 MHz) (808-870 MHz)	S	S	S	S	S	S	S
Encryption Software	O	O	O	O	O	O	
Encryption Hardware	O	O	O	O	O	O	
Multi-Key (Required only if other System Talk Groups are programmed in the radio)	O	O	O	O	O	O	

MOBILE RADIO STANDARDS			
Model Description	**XTL1500**	**XTL2500**	**XTL5000**
Digital		O	O
Dual Mode 800/700 MHz capable	S	S	S
SmartZone		O	O
P25 9600 Software	O	O	O
ID Display		O	O
Encryption Software	O	O	O
Encryption Hardware		O	O
Multi Key (Required only if other System Talk Groups are programmed in the radio)		O	O
Remote Control Head		O	O

S = Standard Feature
O = Optional Feature

5. Recommended Procedures:

N/A

6. Management:

The System Managers are responsible for seeing that the defined standard is followed and maintained.

STANDARD OPERATING PROCEDURES (SOP)

800 MHz Trunked Regional Public Safety Radio System
Standards, Protocols, Procedures

Document Section: 1.7 Sub-Section: Procedure Title: **Radio Auxiliary Equipment** Date Established: 01/04/07 Replaces Document Dated: N/A Date Revised: N/A	RPSCC Radio Sub-Committee Approved Date: 08/02/07

1. Purpose or Objective:

The purpose of this section is to set forth the recommended standards by which all 800 MHz radio users in the regional system will agree to purchase subscriber radios auxiliary equipment that are defined in this standard. This standard is to ensure that radios that are not in compliance do not affect the radio system. These standards will be revised once the RPSCC has purchased and implemented a new APCO P25 700 MHz radio system and the radio model types have been identified to work with the P25 radio system.

2. Technical Background:

- **Constraints**

Radios must meet the recommended standards as set forth when auxiliary equipment is needed by the individual radio subscriber to perform their job. These standards identify the proper radio auxiliary equipment to be used in conjunction with the radio subscriber's model type.

3. Operational Context:

All radios must meet these specific requirements for antennas and batteries when installed on a subscriber's radio. Failure to utilize the manufacturer's recommended standards for the radio auxiliary equipment may cause Law Enforcement and/or Fire Rescue field force personnel to experience static, interference or audio communication breakdown with their assigned Dispatchers. While it is recognized that it is desirable to utilize the accessories manufactured by the radio manufacturer, there are alternative after-market accessories that provide performance equivalent to the manufacture's items, or functionality not available from the Original Equipment Manufacturer (OEM). The permissibility of these after-market items shall be determined by the System Manager after performing a technical evaluation to insure a performance level equivalent to the OEM items.

4. Recommended Protocol/Standard:

In order to meet these requirements the following information describes the minimum standards that must be considered when new auxiliary radio equipment is purchased.

Antennas: Radio antennas shall be either the OEM part or an equivalent as determined by the System Manager. No antenna shall be used that is not pre-approved. In no cases shall "cellular" or shortened stubby designs be permitted unless technical testing confirms that the radiated energy is within 1 dB of the OEM antenna radiation. Testing shall be performed under the direction of the System Manager, not the end user.

Batteries: The battery is the life-blood for the radio and can have a major impact on the radio performance over the course of a shift. It is encouraged that each Public Safety user will have a spare charged battery available. In car charges are an option, either the OEM version or the AdvanceTec model as appropriate for the radio model in use. These shall only be utilized to charge the spare battery. It is highly encouraged that OEM batteries be utilized as they have proven to present fewer quality and performance issues then many of the after-market products.

After-market batteries shall be evaluated prior to implementing their use. Testing shall include fit and finish, drop tests, vibration, cycle capacity, long-term capacity and self-discharge after the battery has been in use for six (6) months. Testing shall be on a representative sample of the after-market manufacturer's product.

Speaker/Microphones: Speaker/Microphones come in two basic styles; Public Safety – equipped with an antenna; Standard – usually equipped with a coiled cord and does not have antenna. The radio system coverage is predicated upon the use of a Public Safety microphone with the appropriate antenna installed on the microphone. Use of Standard speaker/microphones for users that ride in vehicles is discouraged due to the significant range reduction caused by having the antenna below the vehicle glass level and shielded by the vehicle's construction. They may be utilized by bicycle and motorcycle units with the understanding that when radio user is in a vehicle, the coverage may be significantly reduced.

Surveillance kits such as the two or three wire kits, and ComPorts also utilize the antenna mounted on the radio. The same in vehicle coverage issues apply to these units

After-market microphones, surveillance kits, etc. require technical evaluation by the System Manager before they are promoted to the end users.

The following are the manufacturer's recommend standard specific to radio models MTS2000 (antennas only), XTS3000 and XTS5000 (batteries only)

series.

Antenna:

- 806 – 870 MHz – ½" Wavelength Whip (MTS2000 only)
- 806 – 941 MHz – ¼" Wavelength Whip (MTS2000 only)

Public Safety Microphone (Models MTS2000, XTS3000 and XTS5000):

- Straight Cable 30 inches
- Straight Cable 24 inches
- Straight Cable 18 inches
- Command Shoulder Speaker (water-proof) microphone

Batteries for Portable Radios (Models MTS2000, XTS3000 and XTS5000):

- Nickel-Cadmium 7.5 volt Battery (MTS2000)
- Ultra-High Capacity Battery (MTS2000)
- High Capacity NiCD
- High Capacity NiCD FM
- High Capacity NiMH
- High Capacity NiMH FM
- High Capacity NiMH Rugged FM
- High Capacity Lithium Ion
- NiCAD (State approved)

5. Recommended Procedures:

All Antennas, Public Safety Shoulder Mics and Batteries must meet the specifications identified in this standard, protocol and procedures. It is strongly recommended that all after-market vendors work through the System Managers to present their products for evaluation before they contact the end users. End users shall refer all vendors to their System Manager before entertaining the use of an after-market product that connects to, attaches to, or otherwise involves the subscriber units and/or the radio system.

6. Management:

The System Managers are responsible for seeing that the defined standard is followed and maintained.

STANDARD OPERATING PROCEDURES (SOP)

800 MHz Trunked Regional Public Safety Radio System
Standards, Protocols, Procedures

Document Section: 1.8 Sub-Section: Procedure Title: **Talk Group Names** Date Established: 01/04/07 Replaces Document Dated: 08/02/07 Date Revised: 04/08/08	RPSCC Radio Sub-Committee Approved Date: 04/08/08

1. Purpose or Objective:

The purpose of this section is to set forth the principals by which all radio users in the regional system will establish names for **Talk Groups (TG)** and to facilitate intuitive understanding of the TG name. The TG naming standard is also essential because, in keeping with the regional interoperability concept, some TG's will be shared by multiple agencies.

2. Technical Background:

All TG names programmed in the County's 800MHz Trunked Radio System must be unique and consistent from Zone Manager to subscriber. Due to the fact that the newer subscriber units will have a maximum of twelve (12) characters on their display, TG length will be limited to a maximum of twelve (12) characters. When possible, subscriber TG will be consistent with the console database and zone controller. Any subscriber with less than eight (8) characters display will be handled on a case by case basis.

3. Operational Context:

With the exception of the first four (4) characters (see Appendix A), the System Managers are technically free to choose any unique name they wish for TG's assigned within their partition (maximum of twelve (12) characters). The NPSPAC Mutual Aid conventional TG's are assigned a name that is known nationwide. When possible, subscriber TG will be consistent with the console database and zone controller. Any subscriber with less than eight (8) characters display will be handled on a case by case basis.

4. Recommended Protocol/Standard:

The first two characters of the TG alias identify the talk group governing entity/municipality (see Table 1). The third character identifies the department/agency within the governing entity/municipality (see Table 2). The fourth character will have a dash (-) as a separator. The remaining available

characters will be used to complete the talk group alias. It is important to note, depending on the subscriber type and/or model, character display may be smaller or larger. Subscribers units with displays smaller than twelve (12) characters will require condensing the TG name to fit within the display. Any subscriber displays that are under eight (8) characters will be handled, by the Radio System Administrator, on a case by case basis.

It is understood that there is currently a wide variety of subscribers out in the field. In addition to this, there are many agencies who still wish to continue to identify zone and channel assignments prior to the TG in the subscriber unit. Even though the concept that the TG's are to remain consistent from zone controller up to the subscriber is fully supported by OCT, this may be too big of a challenge to overcome at this time. We have come to the understanding that if the agency wishes to continue to identify zone and channel assignment prior to the TG name in the subscriber, they have this ability if they can leave the TG name consistent, as it appears in the zone controller, as much as possible.

5. Recommended Procedures:

N/A

6. Management:

The System Managers are responsible for seeing that the defined standard is followed and maintained.

Appendix A

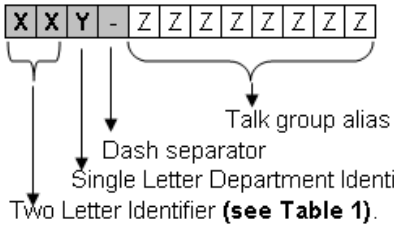
Purpose:

The following is required in order to standardize and document talk group naming convention for the Broward County SmartZone 800Mhz Trunked Radio System.

Description:

The first two characters of the talk group alias identifies the talk group governing entity/municipality. The third character identifies the department/agency within the governing entity/municipality. The fourth character will have a dash (-) as a separator. The remaining available characters will be used to complete the talk group alias. It is important to note, depending on the subscriber model, character display may be smaller or larger. Any subscriber displays that are under eight (8) characters will be handled, by the Radio System Administrator, on a case by case basis. See examples below.

Example 12 character display

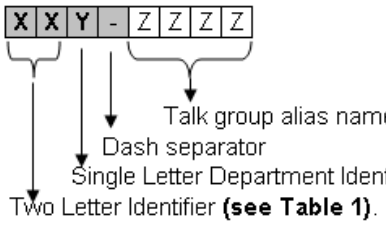


example: B S 0 - D I S P - 4 A = PSB/BSO dispatch channel "Disp4A"

example: F L P - D I S T - 1 = FTL dispatch channel "Dist-1"

Note: Depending on the subscriber model, character display may be smaller or larger. There is a max of twelve (12) characters allowed for talk group alias names.

Example 8 character display



example: B S 0 - D S P 4 = PSB/BSO dispatch channel "Disp4A"

example: F L P - D S T 1 = FTL dispatch channel "Dist-1"

Note: Depending on the subscriber model, character display may be smaller or larger. There is a max of twelve (12)

Tables

Table 1	
BC	Broward County
BS	Broward Sheriff Office
CC	Cooper City
CK	Coconut Creek
CS	Coral Springs
DN	Dania
DR	Deerfield
DV	Davie
FL	Fort Lauderdale
HA	Hialeah, Miami Dade Cty.
HD	Hallandale
HW	Hollywood
LH	Lauderhill
LL	Lauderdale Lakes
LP	Lighthouse Point
LS	Lauderdale by the Sea
LZ	Lazy Lake
MC	City of Miami, Miami Dade Cty.
MB	Miami Beach, Miami Dade Cty.
MD	Miami-Dade County
MG	Margate
MM	Miramar
NL	North Lauderdale
OP	Oakland Park
PC	Palm Beach County
PB	Pompano Beach
PD	Parkland
PK	Pembroke Park
PL	Plantation
PP	Pembroke Pines
SF	State of Florida
SM	Seminole
SN	Sunrise
SR	Sea Ranch Lakes
SW	Southwest Ranches
TM	Tamarac
WM	Wilton Manors
WP	West Park
WS	Weston

Table 2	
A	**Airport**
B	FUTURE USE
C	**Communications**
D	FUTURE USE
E	**Port Everglades**
F	**Fire Rescue**
G	FUTURE USE
H	FUTURE USE
I	FUTURE USE
J	FUTURE USE
K	FUTURE USE
L	**Local Government**
M	**Mutual Aide**
N	FUTURE USE
O	Office*
P	**Police**
Q	FUTURE USE
R	**Parks & Rec**
S	**School**
T	FUTURE USE
U	FUTURE USE
V	FUTURE USE
W	FUTURE USE
X	FUTURE USE
Y	FUTURE USE
Z	FUTURE USE

*** To be used only by Broward Sheriff's Office**

STANDARD OPERATING PROCEDURES (SOP)

800 MHz Trunked Regional Public Safety Radio System
Standards, Protocols, Procedures

Document Section: 1.9 Sub-Section: Procedure Title: **Shared Use Of Talk Groups** Date Established: 01/04/07 Replaces Document Dated: N/A Date Revised: N/A	RPSCC Radio Sub-Committee Approved Date: 08/02/07

1. Purpose or Objective:

The intent of this standard is to provide an option to the users of the 800 MHz system, which will allow the talk group owners to "at their discretion" predefine sharing authorizations for other agencies.

2. Operational Context:

Talk Groups are considered to be "Owned" by the agency requesting the creation of the Talk Group, similar to the ownership that applies to conventional RF resources. As the owner of the Talk Group the owning agency has the authority and control to define who can and cannot use the Talk Group and to what "degree. Traditionally this process has been primarily accomplished with "letters of authorization."

The optional method to simplify this process is for the owning agency to predefine sharing authorization, as diagrammed in the table example below.

The predefined authorizations would be kept in the Talk Group spreadsheet maintained by the System Managers. These spreadsheets would be shared between the System Managers, and would be a reference available for Talk Group planning. If an agency does not pre-define sharing authorization for a particular talk group, the default will be a "P" as defined below.

3. Recommended Protocol/Standard:

The use of the following codes, which are combined to define the intended pre-authorizations…

P = Permission is required to gain authorization for use. A letter of permission must be generated from the System Manager of that agency that wishes to use another agency's Talk Groups for their radio subscribers and/or their Dispatch consoles and this written request must

be sent to the System Manager of the system that has ownership of those Talk Groups for their system.

D = Defined agencies may share, to be defined in a separate letter. The letter would outline specific purpose talk groups, i.e., only dispatch consoles, only neighboring cities, etc. The letter will be on file with the appropriate System Managers.

L = Like agencies may share, "Fire, Medical, Law, Public Works, etc."

A = All agencies.

RX = Only authorized to receive.

TX = Authorized to transmit and receive.

4. Recommended Procedures:

The System Managers, working with the user groups, would perform this task.

5. Management:

The System Managers are responsible for the management of this procedure. The larger table is also used to layout the Fleetmap information as described in this manual in Section 1.1, Fleetmap Standards.

Talk Group	Owning Agency	Description	Administrating Agency	Global Sharing Authorizations P = Permission letter required to gain authorization for use D = Defined Use – Letter required L = Like agencies may share "Fire, Medical, Law, Works" etc. A = All agencies RX = Are only authorized to receive TX = Are authorized to receive & transmit
Talk Group 1				D-TX
Talk Group 2				L-TX
Talk Group 3				A-TX
Talk Group 4				P-RX
Talk Group 5				P-TX
Talk Group 6				D-TX
Talk Group 7				L-TX
Talk Group 8				A-TX

Talk Group 9				P-RX
Talk Group 10				P-TX
Talk Group 11				D-TX
Talk Group 12				L-TX
Talk Group 13				A-RX
Talk Group 14				P-RX
Etc.				P-RX

The “RX” option shown in the table is an authorization that permits receive only use, although the radio would be technically capable of transmit (TX) operation on the talk group.

STANDARD OPERATING PROCEDURES (SOP)

800 MHz Trunked Regional Public Safety Radio System
Standards, Protocols, Procedures

Document Section: 1.10 Sub-Section: Procedure Title: **Scanning Talk Groups** Date Established: 01/04/07 Replaces Document Dated: N/A Date Revised: N/A	RPSCC Radio Sub-Committee Approved Date: 08/02/07

1. Purpose or Objective:

This procedure is to identify operational procedures and responsible authorities governing Scanning activities as it relates to the Scan function in the individual subscriber radio.

2. Technical Background:

- **Capabilities**

  The network infrastructure and subscriber units need to be configured to permit managed user Scanning of Talk Groups. Whether or not Scanning will be utilized in subscriber radios, it is at the option of the user agency. Users also need to be trained that merely including a Talk Group in a non-priority Scan list will not necessarily result in the user hearing traffic on that Talk Group. The Talk Group must also be "active" at the site where the user is affiliated. Talk Groups are active on a site if the Zone Controller is programmed to allow the Talk Group to appear on that site and there is at least one user affiliated at the site which has the Talk Group of interest as their selected channel.

- **Constraints**

  How the radio is programmed to handle wide area and local sub-system Talk Groups will determine priority Scan capabilities. If the local sub-system Talk Groups is not programmed to the same "system" in the radio, they cannot be included in the priority monitor Scan list. In this case, only Talk Group Scan can be implemented. Priority Scan requires System Infrastructure configuration in order to perform as expected. The Talk Groups that are deemed to be Priority Monitor Groups need to be configured as such by the System Managers. There are practical limitations on the overall number of Priority Monitor Groups that can be enabled due to the amount of time required to distribute the list of active Talk Groups to the radios in real-time. Talk Group Scan does not provide

a priority feature to direct the radio to the priority Talk Group. Talk Group Scan can Scan Talk Groups from different systems (as defined in the radio internal programming) and conventional channels. It is strongly recommended that "talkback Scan" not be used. Talkback Scan would direct the user to transmit on the last active Talk Group the radio heard traffic on. This will cause confusion as the radio user will not know what Talk Group the radio will be transmitting on as it will constantly change based upon what the radio last received. Scan is not recommended for those users that must hear critical communications.

While Scanning will be available on the systems it will necessarily be limited and, therefore, not be as robust as in conventional radio systems.

3. Operational Context:

The network infrastructure and subscriber units will be configured to balance the ability for users to achieve wide area coverage where necessary, and maintain an acceptable level of service for all users. The use of "Critical User" and "Critical Site" in the system for the purpose of non-priority Scanning is not permitted and Scanning between different sites will be accomplished by the use of "requested sites."

Before priority Scanning is allowed on an individual subscriber's radio, it must be pre-approved by the agency's management and/or command.

Additionally, priority Scanning of Talk Groups must be evaluated by the System Manager to make sure the radio system is not affected by the use of this feature.

4. Recommended Protocol/Standard:

Limited Scanning/monitoring privileges may be pre approved by the affected Talk Group owners and System Managers.

Before Scanning of owned Talk Groups, permission must be granted. permission must come from:

- The System Managers of the sites that are being requested for the Talk Group
- The jurisdiction/agency who is the "owner" of the requested Talk Group

Mutual aid, special roaming and other shared Talk Groups may be Scanned at any time; however, "requested site" determinations will be made by the System Managers of the affected sites.

5. Recommended Procedures:

Permission:
If the Talk Group does not appear on the approved Scanning list, permission must be obtained in writing from the Talk Group owner and the System Manager of the non-home site or sites being "requested" if applicable.

Scanning Configuration:
If trunked Scanning is desired, it is recommended that Scanning should normally be limited to owned trunked Talk Groups which are affiliated with their "always preferred site(s)".

It is further recommended that Scanning normally be disabled when the user leaves the system and switches their radio to a conventional (non-trunked) channel. However, if mixed mode Scanning (both trunked Talk Groups and conventional channel members) is required by some users, it is also recommended that this Scan type only be available when the radio is selected to a conventional channel. This is because mixed mode Scan does not provide priority reverts and the user will typically miss substantial portions of conversations on the selected channel. Talkback Scan is highly discouraged, as the user cannot control the Talk Group used to transmit. Can lists can be either programmed into the radio with no user access for changes, or the list can be made accessible for user modifications. It is preferred that the list is made user configurable to allow those users that can handle Scan to determine what they want to listen to and make changes "on the fly" as their requirements change.

Scanning of Non Home Site Talk Groups:

It is possible to monitor a non home Talk Group by configuring the system to request the desired non home Talk Group appears on your primary/home system or "always preferred site(s)". Doing so however, will consume a repeater channel on your primary/home system or "always preferred site(s)" and will carry the requested non-home Talk Group priority setting with it. Also, a call on the requested non-home Talk Group will not be delayed (busy queued) if the home system or "always preferred site(s)" does not have a channel available. This however may cause unacceptable conditions where the majority of users do not receive the call while the dispatcher or calling party has no indication that a large segment of their users did not receive the call. While this "requested site" is the recommended approach, it must be carefully controlled, monitored and evaluated due to the potential to exhaust system resources. It must be approved by the affected System Managers.

6. Management:

The System Managers will be the final authority for controlling the Scan feature and Scanning issues. The agency's management and/or command will have the authority to approve/disapprove this feature for their users.

STANDARD OPERATING PROCEDURES (SOP)

800 MHz Trunked Regional Public Safety Radio System
Standards, Protocols, Procedures

Document Section: 1.11 Sub-Section: Procedure Title: **Emergency Button** Date Established: 01/04/07 Replaces Document Dated: N/A Date Revised: N/A	RPSCC Radio Sub-Committee Approved Date: 08/02/07

1. Purpose or Objective:

There will be a large variety of users on the radio system with various Emergency Button needs. The various ways the emergency key can be configured will allow for flexibility of use, however, it is important to design the system in such a way that when an Emergency Button is pushed, it is responded to quickly and appropriately.

2. Technical Background:

- **Capabilities**

  The "Emergency Button" feature, if it is programmed into the subscribing agency radios, will allow a radio user to send an emergency notification by pressing the specific Emergency Button on the radio. The notifications will audibly and visually alert all dispatch console positions that have the talk group up that the emergency notification is routed to. Other radios that have the talk group selected will also receive the emergency notification, and display the radio ID of the radio generating the emergency. The display of an ID is dependent upon radio model, firmware version, and purchased options. The user activating the Emergency Button has the obligation to properly cancel the activation by pushing – and holding the Emergency Button until a continuous tone sounds. Failure to properly cancel the alarm on the originating radio will cause a new alarm activation each time the user transmits.

  Emergency calls are also automatically assigned the highest priority available and would be the first available from the queue if the system is in a busy situation. Subscriber's radios can optionally be configured to automatically activate the Push-to-Talk (PTT) for a programmed period of time if the Emergency Button is pressed.

- **Constraints**

Consider two situations a fire department engine company could be faced with, that show different operational needs:

1. An engine company responds to a medical at a private home. Upon entering the home, they are met by an out-of-control person who fires a handgun at them.

2. An engine company is conducting an interior fire attack when the floor collapses, trapping them in the basement.

In the first example, a firefighter may push his Emergency Button as he is running out of the home. He may want it to signal his dispatcher on the main talk group. The dispatcher would immediately see the signal, assess the situation, and send the police to assist.

In the second example, a firefighter may push his Emergency Button, and have it send the signal on his fire ground operations channel. The on-scene safety officer would attend to this signal by immediately sending in a rescue crew comprised of people already at the scene.

The design should also avoid the instance where an Emergency Button is pressed, and nobody can identify the user, or the wrong people attend to the emergency. Such a situation would occur if a police officer's Emergency Button were configured to signal on a Main Channel talk group. In that case, pressing his Emergency Button would probably signal every police dispatch console on the radio system.

Another example is that a public health official pushing the button when alone in a dangerous situation. If the public health official's radio were configured to signal on the County COUNTY main dispatch talk group, but is unknown to the dispatcher, the dispatcher may be confused by who is in distress, and may not know how to respond. This example shows the importance of an agreement between the central monitoring agency and the radio user agency.

Emergency Button programming cannot be configured on a talk group by talk group basis. This function is defined within the radio personality consisting of a group of 15 talk groups. The personality may be configured to direct the radio to a specific talk group or to use the current selected talk group of the talk groups within the personality. Emergency Button configuration requests shall be discussed with the System Manager of the affected System as radio programming codeplugs are impacted.

It is recommended that non-Public safety, i.e. Public Service, or general government, users not have the Emergency Button functionality unless

appropriate training and monitoring resources are available to respond to the alarms. Non-public safety emergency alarms shall not be directed to a Public Safety Talk Group unless the Public Safety Dispatch Center responsible for the Talk Group agrees to assume responsibility for the alarms.

3. Operational Context:

An Agency may choose to utilize the Emergency Button functionality, or to disable its use. If an Agency chooses to use the Emergency Button it shall be utilized as an indication of an immediate threat to life or property. Use of the Emergency Button to advance a routine Talk Group call in the priority cue is not an accepted usage. Agencies may choose to have the emergency activations occur on a primary dispatch Talk Group, or be directed to a specific Talk Group set aside to handle Emergency Activations. Agencies that may have access to the Talk Groups from other Agencies in their consoles will receive the emergency activation notifications if that Talk Group is active in a folder in the console operator position. Agencies shall NOT acknowledge/silence/cancel emergency activations from another Agency without contacting that agency before taking action. To do so may cause a valid emergency alarm to go unanswered.

Any Agency that acknowledges/silences/cancels emergency activations from another Agency more than 3 times, without contacting that agency before taking action, shall remove the other Agency Talk Groups from their consoles within 30 days of receiving notification from the Talk Group owner or System Manager.

Subscriber units that send an excessive number of false emergency alarm activations shall be located and corrected by the subscriber owner agency as expediently as possible. Excessive is determined to be four (4) or more false alarm activations within a 24-hour period. The subscriber owner agency shall take all steps necessary to locate and correct the false activations. There are circumstances where it is not possible to stop the false activations by attempting to inhibit the radio or by removing the radio authorization record from the system databases. In these cases the radio must and shall be located by the Owner Agency and brought to the servicing vendor for repairs within 30 days of the first false activation. Dispatch Centers shall report all instances of excessive false emergency alarm activation to their System Manager. The report shall include the date, time and Talk Group the emergency occurred on, along with either the subscriber alias or displayed radio ID #.

4. Recommended Protocol/Standard:

Use of the Emergency Button as an emergency signaling option should be available to any agency on the radio system, subject to certain conditions and provisions.

1. Agencies are not required to use this capability of the radio system.
2. No agency will be permitted to enable their emergency signal on a talk group designated as “emergency restricted.”
3. All agencies implementing the Emergency Button must have a plan in place to respond to an Emergency Button activation.
4. All Emergency Button response plans must include, at minimum:
    - A central radio monitoring point that can identify which radio user pushed the button, the location and nature of the emergency and what the proper agency response should be
    - A central monitoring point must be available during any/all hours that personnel are using the radio system.
    - A policy for use of the Emergency Button by radio users.
    - A response plan to assist the radio user in need.
    - In the event the central radio monitoring point is not the same agency as the radio user, an agreement on policy, monitoring, use and response must be in place among the agencies.
    - Where available the orange button should be used to program the Emergency Button.

5. Recommended Procedures:

N/A

6. Management:

Agencies wishing to use the Emergency Button function must coordinate which agency resources that will be receiving the emergency calls, the receiving agencies must have an appropriate plan in place, and documented as to the process that they will use to handle the emergency calls.

STANDARD OPERATING PROCEDURES (SOP)

800 MHz Trunked Regional Public Safety Radio System
Standards, Protocols, Procedures

Document Section: 1.12 Sub-Section: Procedure Title: **Encryption** Date Established: 01/04/07 Replaces Document Dated: N/A Date Revised: N/A	RPSCC Radio Sub-Committee Approved Date: 08/02/07

1. Purpose or Objective:

This procedure is to identify operational procedures and responsible authorities governing Encryption activities.

2. Technical Background:

- **Capabilities**

  The network infrastructure and subscriber units need to be configured to permit Encryption of selected Talk Groups. Whether or not Encryption will be utilized in subscriber radios, it is at the option of the user agency. Users also need to be trained to know how to activate the Encryption feature when needed on a specified talk group.

- **Constraints**

  It will be the subscriber radio user's responsibility to activate the Encryption feature when needed. In most cases the use of Encryption will be decided once a talk group is dedicated to the use by the personnel in the field that are involved in the operational situation.

  The Encryption feature blocks all non-approved/intruder radio users and scanners from hearing the conversation of the talk group that is being used for the situation. At this point in time (2007), only the City of Hollywood and County of Broward infrastructure support Encryption capabilities. Encryption can only occur on a digital capable talk group. Both the availability of digital Talk Groups and digital subscriber IDs is limited and must be coordinated with the System Managers prior to any desired implementation. Currently only DES-OFB and DES-XL Encryption algorithms are supported. Encryption Talk Groups that must appear on a console will need to have Encryption key loaded into the Console DIU. This has the potential to reduce the security of the talk group as others may be able to access the clear audio via a console.

3. Operational Context:

The Encryption feature needs to be pre approved by the agency's upper level management. Police units that are approved to receive Encryption for their subscriber radios are designated as SWAT, K-9, Homeland Security and Special Investigation Division, and any other unit as determined by the Department. Other Departments and Divisions such as the Fire Department may choose to encrypt some or all of their Talk Groups as needed to insure operational security.

4. Recommended Protocol/Standard:

Limited Encryption privileges may be pre approved by the affected Talk Group owners and System Managers.

Before allowing Encryption as a feature of a subscriber radio user of owned Talk Groups, permission must be granted. Permission must come from:

- The System Managers of the sites that are being requested for the talk group
- The jurisdiction/agency who is the "owner" of the requested talk group

5. Recommended Procedures:

A subscriber radio user that has the Encryption feature will be responsible for activating/deactivating it as needed. Talk Groups may also be "strapped" secure in the subscriber programming to permit only encrypted operation if desired.

Encryption Keys shall be maintained by the Agency utilizing the Encryption feature. Each agency is responsible to insure that they do not duplicate Logical IDs (LIDs). Logical IDs for the keys consist of a four-digit number entered as the last four digits of the Key. LIDs for Broward County shall be in the 1000 series, Deerfield Beach shall use 2000, Hollywood shall use 3000, Fort Lauderdale and Pompano Beach shall use 4000, and Plantation shall use 5000. As other systems are brought into the Regional Public Safety Communications System, their LIDs shall start with the site number for their infrastructure. This structure insures that there will not be duplicated LIDs which will cause problems when utilizing Encryption in the integrated environment that we share. The first 16 digits of the key are at the discretion of the Agency.

There are two shared Regional Special Investigations Joint Operations Talk Groups that utilize a shared common key. These two Talk Groups may not be utilized on a permanent basis for any one specific unit or agency. They are common, shared resources dedicated to interagency operations. The talk group information and key are available to authorized personnel by contacting either the System Managers of the Broward COUNTY's Office and Fort Lauderdale.

6. Management:

The System Managers group and the agencies upper level management will be the responsible authority for Encryption issues.

STANDARD OPERATING PROCEDURES (SOP)

800 MHz Trunked Regional Public Safety Radio System
Standards, Protocols, Procedures

Document Section: 1.13 Sub-Section: Procedure Title: **Definitions & Acronyms** Date Established: 06/28/07 Replaces Document Dated: N/A Date Revised: N/A	RPSCC Radio Sub-Committee Approved Date: 08/02/07

1. Purpose or Objective:

To clarify terms used throughout the standards, protocols and procedures manual. All definitions will be found in this section.

2. Management:

Should there be additions, deletions or changes to these procedures the Regional Public Safety Communications Committee (RPSCC) members are responsible for revising this section.

3. Definitions (in alphabetical order)

APCO P25 Compliant: Public safety equipment that meets (Association of Public Safety Communications Officials) APCO P25 standards.

Announcement Group: is a collection of Talk Groups.

Audit: An audit is defined as a one time, infrequent or occasional in depth analysis of comprehensive elements. An audit may be annual or upon demand. An audit may be stimulated by an event or complaint of monitoring outcome.

"Common" or "Pool" Talk Groups: Common/pooled talk groups (TG) are those that are set-aside for communicating across multiple agencies. Agency radio users in appropriate service areas who need to talk to one another for day to day business or for mutual aid will all put the appropriate common or pool talk group in their radios to be available in time of need. Example: Fire Departments will all have the common Statewide Fire Mutual Aid TG in their radios. "Pool" is distinguished from "common" in that pool implies more then one, such as TAC 1 – 4 is a pool of common regional tactical TGs for law enforcement.

Failsoft Signaling: During normal system operation, the central controller supplies the base station's Failsoft circuit with a Transmit Data (TDATA) signal. The TDATA signal consists of an OSW followed by an LSHS signal, followed by

a Disconnect Word signal. The TDATA signal keeps the base stations in the trunking mode. If TDATA transmission stops because of failure of the central controller, the base stations revert to the Failsoft mode.

- The base station unmutes and transmits a Failsoft data word
- Radios respond to the Failsoft word and unmute, allowing service to continue via community repeater type operation.
- The base station sends out a 900 Hz tone for 280 milliseconds every 10 seconds to alert the radio user that the system is in Failsoft mode.

Logging: Audio recording of a radio communication.

Mission Critical Operations: Those governmental, quasi-governmental and non-governmental operations carried out by authorized users which are reliant upon a functioning two-way radio communications system which unavailability, degradation, delay or failure, partial or complete, would significantly impact or impair the successful delivery of a vital service or mission. Operations would include, but are not limited to the categories below:

- Public Safety – Those functions of government that exist to protect the physical well being of the public as a whole from physical danger – continuous delivery of essential public services. Included with this group are Legal Counsel and SHERIFF's Special Investigative Unit (SIU) and the Administration Site Operations.

- Transportation – Those functions of the government that exist to provide safe, effective and efficient multi-mode movement of the public commodities including public roads, highways, waterways, railways, airways and public transportation systems. Included with this section is the Broward SHERIFF buses that may need to be used as a back-up to the Broward County Mass Transit buses should a mass evacuation occur due to a major incident.

- Environmental Protection – Those functions of the government that exist to protect the environmental from changes that are detrimental to the existence and continuance of that environment.

- Public Works – Those functions of the government that provide "first responders" that may be necessary to clear streets and highways so that Public Safety operations can be conducted after a major event like a hurricane.

Mobile Radio: A station in the mobile service, generally installed in a vehicle, intended to be used while in motion or during halts at unspecified points.

Mobile Service: A service of radio communication between mobile and base

stations, or between mobile stations.

Monitor: Monitoring is defined as the scheduled and routine inspection of operational practices and facilities and/or the review of system reports and documents. Monitoring frequency would generally be on a predetermined, scheduled basis

Non-Critical Operations: All other governmental, quasi-governmental and non-governmental operations, which are reliant upon a functioning two-way, radio communications that do not meet the above mission critical or department critical definitions.

Operational Fixed Station: A fixed station, not open to public correspondence, operated by, and for the sole use of those agencies operating their own radio communication facilities in Public Safety, Industrial, Land Transportation, Marine or Aviation Radio Services.

Patch:

Permanent (hard) Patch: A patch between two or more audio resources on a system, which is fixed and cannot be controlled or edited by the dispatcher.

Manual (soft) Patch: A patch between two or more audio resources on the system, which is setup and controlled by the dispatcher. The dispatcher owning the patch can add and delete resources as needed.

Portable Radio: A radio that is completely freestanding and may be hand-carried or worn by the radio user.

Preferred Site Assignment: A SmartZone system can also be configured with Preferred Site Assignment operation. This feature allows radio users to maintain conversations on sites especially useful to operations and group requirements. In areas with overlapping coverage, radios will work on their preferred site in order to efficiently utilize channel resources while minimizing the number of channels necessary to complete a talkgroup call. Four types of preference can be programmed into the radio personality:

- **Always Preferred –** The subscriber unit will always use this site if it has at least acceptable signal strength, even if the site enters site trunking mode.
- **Preferred -** The subscriber unit will use this site if it has at least an acceptable signal strength rating and is in wide-area trunking mode.
- **No Preferred Site –** This is the default setting for subscriber radios. The subscriber unit will use the best signal according to the best Receive Signal Strength Indication (RSSI).
- **Least Preferred –** The subscriber unit will avoid this site unless no other sites with at least acceptable signal strength are available for use.

Private Call: This allows one radio user to talk to and be heard by only one other radio user. This feature allows a supervisor to discuss confidential matters with a particular member of a talkgroup while other members of the same talkgroup remain squelched.

Public Safety: All Law Enforcement / COUNTY, Fire, Emergency Medical and related service areas. These include badged and/or sworn ancillary personnel such as Park Rangers, Court Security Officers, Community Corrections, and those who support public safety operations under special circumstances.

Public Safety Answering Points (PSAPs):

Primary: The PSAP where a 9-1-1 call is originated and received by a call taker then transferred to a dispatcher for dispatching police, fire or emergency medical assistance.

Secondary: The PSAP that receives transferred 9-1-1 call taker calls and is then dispatched and monitored from this center.

Public Service: Public Service in this context refers to general government personnel such as Public Works, Transportation, and other similar public service operations.

RF: Radio Frequencies

Regional Public Safety Communications Committee (RPSCC): The governing body of municipal Police and Fire Chief's, IT Management and decision-making staff that are empowered to develop Standards, Protocols and Procedures regarding the intent to accomplish the Broward County's Charter direction to achieve regional communication plans to establish Radio Interoperability and Closest User Response objectives.

Region 7: State of Florida Homeland Security region that is made up of Broward, Dade, Monroe and Palm Beach Counties.

Regional System: In this context of this manual this term is intended to represent the entire Region-wide 800 MHz Public Safety Communication System.

SmartZone Trunked System: The 28 channel trunked radio system that serves public safety communication users in a wide-area coverage network. This system allows for roaming from one radio system to another trunked or conventional system seamlessly and provides communications back to the municipality's home based dispatch center. This system can operate in an analog or digital mode.

SmartZone Manager Terminal: The resource tool that is used by System Managers to administer their radio system for maintenance issues and controls of how their radio subscriber and consoles are configured / programmed.

Subscriber Radio: A portable radio that is assigned to a specific individual or a mobile radio that is shared by multiple staff that drives and operates the vehicle.

System: A countywide public safety radio communication system that consists of a shared region-wide infrastructure, the elements of which are identified in the Regional Public Safety Communications Plan and Subsystem integrated into or interconnected by the shared countywide network.

System Manager/ Administrator Positions:

- System Manager – individual in charge of the radio system of a participating agency.

- System Administrator – individual who is responsible for the day to day radio system operations of a participating agency.

- Sub-System Administrator – individual who is responsible for the day to day radio sub-system operations of a participating agency.

- Contract Manager – Director of BSO Communications Technology or his appointed designee.

Talk Group: The Talk Group is the primary level of communication in a Trunked radio system. This provides the effect of a private channel down to the talkgroup level and prevents members of one talkgroup from hearing the talkgroup calls generated by radios in other talkgroups.

Telephone Interconnect: The use of a radio to make a two-way call between two radios subscribers when privacy is needed to block other radio subscribers from hearing the conversation. This feature must be programmed in the radio and activated on the system in order for it to be functional.

Variance: An allowed divergence from full adherence of an adopted standard, protocol or procedures

Waiver: A complete release from an adopted standard, protocol or procedure.

4. **ACRONYMS (in alphabetical order)**

ALS - Advanced Life Support

ATAC	-	All (user) Tactical talk group for 800 radios
AVL	-	Automatic Vehicle Locator
APCO	-	Associated Public Safety Communications Officials
BLS	-	Basic Life Support
CEB	-	Central Electronics Bank
CTCSS	-	Continuous Tone Coded Squelch System
DIU	-	Digital Interface Unit
DTMF	-	Dual Tone Multiple frequency
EDICS		Emergency Deployable Interoperability Communications System
EMS	-	Emergency Medical Services
EMRS	-	Emergency Medical Radio System
FCC	-	Federal Communications Commission
ICALL	-	International 800 MHz Calling Channel
ITAC	-	International 800 MHz Tactical Channel
MHz	-	Megahertz
NAEMSD	-	National Association of State EMS Directors
NPSPAC		National Public Safety Planning Advisory Committee
PSAP	-	Public Safety Answering Point
PSWAN		Public Safety Wide Area Network
PTT	-	Push to Talk, i.e. talk button
RF	-	Radio Frequency
RX	-	Receiver of radio communications
SMG	-	System Manager, the owner of the Regional Public

		Radio System and Sub-Systems
RSS	-	Radio Service Software
TX	-	Transmission of radio communications
UHF	-	Ultra High Frequency
VHF	-	Very High Frequency

STANDARD OPERATING PROCEDURES (SOP)

800 MHz Trunked Regional Public Safety Radio System
Standards, Protocols, Procedures

Document Section: 1.14 Sub-Section: Procedure Title: **Console Naming** Date Established: 06/28/07 Replaces Document Dated: N/A Date Revised: N/A	RPSCC Radio Sub-Committee Approved Date: 08/02/07

1. Purpose or Objective:

The purpose of this section is to set forth the principle by which all System Managers / Administrators of the regional system will establish names for the Radio IDs used to support dispatch console positions. This is necessary because IDs are not associated with a Radio User Alias.

2. Technical Background:

Constraints: The serial number field in Radio ID screens in 12 characters long. Every Talkgroup per console position requires a Radio ID programmed for that position, for example a single console position may have 50 radio ID programmed to support that position.

3. **Operational Context:** Every radio in the system represents a radio, but not every Radio ID in the system is a radio, some are consoles. By planning an identification process, we can use the radio serial number field in the radio entry screen in the system to categorize consoles so that they can be easily identified.

4, **Recommended Protocol/Standard**: The Serial Numbers used in the records for console Operator positions will be formatted according to the following:

OPTION 1

- Regional Operating Agencies would have naming prefixes of at least two characters that would stand alone. Counties would be pre-named with a two character identifying mnemonic, and the Cities and Agencies of the Counties would be included under prefix of the County they are in.
- The next three characters would be the letters “con” for console, so as to easily distinguish this identifier from other radio aliases.
- The characters following these first five are at the individual agency’s discretion.

OPTION 2

- Starting with a 2 – digit prefix to identify the Console location “for example FL, PB, HL, etc.
- The next 2 digits represent the CEB number.
- The following 2 digits indicate the TDM slot on that CEB
- The last four characters are to be unique, at the individual agency discretion.

4. Recommended Procedures:

   N/A

5. Management:

   The System Managers / Administrators are responsible for ensuring compliance with the standard.

EXHIBIT H

BSO Responsibility:

Provides the following services to BSO Departments of Law Enforcement (DLE), Detention (DOD), & Fire Rescue:

1. Purchase and order radios and accessories per the standards set forth by COUNTY.
2. Maintain radio inventory and lifecycle of radios to be consistent with COUNTY radio technology.
3. Maintain battery inventory to include deep discharge and re-charge procedures.
4. Tier 1 support for DLE and DOD which is defined as replacement of damaged radio antenna, battery, RF adaptors, external microphone and the exterior cleaning of housing switches. This excludes BSO Fire Rescue.
5. Maintain the fleetmaps for all BSO radio users and provide a copy to COUNTY.
6. Responsible for defining code plug parameters and providing those parameters to COUNTY.
7. Follow the established project schedule and timeline developed by the COUNTY for the completion of re-banding BSO radios.
8. Establish radio programming guidelines and maintain radio programming for confidential BSO radio users which shall include Strategic Investigations, SWAT, Tactical Units and Internal Affairs. This excludes Fire Rescue and Road Patrol among other units.
9. Provide recurring General Fund funding to the COUNTY for the total costs and benefits of one (1) COUNTY employee position to support the programming and maintenance requirements on all BSO user radios. The COUNTY will provide notice to BSO of the total costs and benefits for the one (1) employee position on an annual basis.
10. Upon renewal of contract city's agreement with BSO, BSO will require the contract city to be responsible for COUNTY labor, parts and materials associated with Tier 3 support plan. COUNTY labor rates and all other costs associated with Tier 3 support will be provided to BSO on an annual basis.

COUNTY Responsibility:

1. Tier 1 support for BSO Fire Rescue which is defined as replacement of damaged radio antenna, battery, RF adaptors, external microphone and the exterior cleaning of housing switches.
2. Tier 2 support for BSO radios which is defined as replacement of defective volume or channel select knobs.
3. Tier 3 support which is defined as repairs which require the exterior case of a radio to be opened.
4. Parts and materials required to perform Tier 3 repairs for portable, mobiles, and consolettes.
5. Provide monthly billing report for OCT labor, parts and materials used for Tier 3 support in accordance with item 10 under BSO responsibility regarding contracts with municipalities.
6. COUNTY will write code plugs based on BSO specification for all BSO radio users.
7. COUNTY will perform re-banding for all BSO radios.